CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 21 — SEPTEMBER 2015

The Dark Web Dilemma: Tor, Anonymity and Online Policing

Eric Jardine

THE DARK WEB DILEMMA: TOR, ANONYMITY AND ONLINE POLICING

Eric Jardine

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Eric Jardine joined CIGI as a research fellow in May 2014 in the Global Security & Politics Program. He contributes to CIGI's work on Internet governance, including the CIGI–Chatham House-sponsored Global Commission on Internet Governance. His current research focuses on cyber security, cyber terrorism, cybercrime and cyber protest. He holds a Ph.D. in international relations from the Norman Paterson School of International Affairs at Carleton University, Ottawa, Canada.

EXECUTIVE SUMMARY

Online anonymity-granting systems such as The Onion Router (Tor) network can be used for both good and ill. The Dark Web[1] is possible only because of online anonymity. The Dark Web poses a dilemma. Illegal markets, trolls and online child abuse rings proliferate due to the technology of Tor and other similar systems. However, the anonymity provided by such systems gives cover for people in repressive regimes that need the protection of technology in order to surf the Web, access censored content and otherwise exercise their genuine right to free expression. In other words, Tor is basically a neutral tool that can be used for either good or ill. Whether the technology is worth it, depends upon the net effect. Unfortunately, the costs and benefits of a system like Tor are not evenly distributed globally. The ills tend to cluster in liberal countries, while the benefits tend to cluster most in repressive regimes. Shuttering anonymity networks is not a viable long-term solution, as it will probably prove ineffective and will be costly to those people that genuinely benefit from these systems.

Rather than being a solely technological problem, this paper argues that the issue posed by the Dark Web, enabled by anonymity-granting technologies, is a social one. Just as peace and order are maintained in our offline lives through judicious policing, the same principle should apply online. The networks of the Dark Web need to be more actively policed, especially in liberal democratic countries. Online policing, as shown by the takedown of illegal marketplaces such as Silk Road and child pedophilia rings, is actually possible, and both as effective and as expedient as offline policing. More movement in the direction of judicious online policing can minimize the socially damaging costs of anonymity-granting technologies, while still allowing the benefits of such systems. It is not the ideal solution, but it is likely the best that can be done.

INTRODUCTION

The Dark Net: its very name brings to mind images of shadowy alleys, malicious, hard-faced individuals and socially damaging activity. The Dark Net is a part of the Internet that most people probably do not know how to access, nor want to explore. A special web browser is needed just to reach it.[2] One such browser, embedded in a larger networked system, is the widely used Tor network.[3]

A lot happens via Tor. This paper runs through some of what goes on in the Dark Net, with a particular focus upon how the anonymity of the Tor browser allows for both nefarious and noble undertakings. It uses evidence from a variety of news accounts and secondary literature to detail how anonymity can be used as a tool of those that want to undertake socially damaging activity. It also uses the results of a recently conducted study on Tor usage rates that shows empirically that people in politically repressive countries are often driven to use the anonymity network out of necessity (Jardine, n.d.).

The basic story to emerge from all of this evidence is that an anonymity-granting system such as Tor, as with other technologies, is just a tool. Like fire, a hammer, or a car, the Tor network can both improve life and provide the means to take it away. What matters is not what the technology is, but how it is used and what the net effect turns out to be.

Framed from this perspective, the focus of public debate should move away from demonizing the technology, or looking for quick technological fixes, toward the idea that, like every other aspect of human society, the Dark Net needs to be policed. This recommendation is particularly relevant for liberal democratic countries, where the dark side of anonymity imposes the highest costs and the benefits of Tor are least pronounced. Ideally, policing needs to be undertaken within clearly defined, rule-based limits. That is no different than the rest of society. Sometimes, as the saying goes, the more things change, the more they stay the same.

The next section describes the Tor-hosted Dark Net. Following that, the paper discusses the negative effects generated by the anonymity of the Dark Web. The third section presents new statistical evidence to show that sometimes the anonymous network is used for good. The fourth discusses the policy implications that flow from the dual nature of the technology, in particular, how online policing of the Dark Web has proven to be just as effective as offline policing. The only way forward is to police the Dark Web, just as we police all aspects of society.

1 The Dark Web and the Dark Net are used interchangeably throughout this paper and mean the same thing.

2 The borders of the Dark Web are blurry. See, for example, Chertoff and Simon (2015). For the purposes of this paper, the Dark Web can be defined as a part of the Internet that is only possible because of online anonymity. This definition does not imply that online anonymity is enough to create the Dark Web, only that the Dark Web can't exist without it. In social science terms, online anonymity is a necessary, but not a sufficient, cause of the Dark Web.

3 The Tor browser is the entry point of focus to the Dark Web for this paper, but there are other ways into the Internet's underground. The Tor browser is also one of the main gateways to anonymity in this paper. Again, others exist.

TOR AND THE DARK NET

Under normal circumstances, when you are trying to access the Web, you send a signal from your device across the Internet to the server that hosts the material that you want to view. That can be a cat meme, a pornographic video, a news organization's webpage or whatever else might tickle your fancy. The server then returns the data to your device. The relationship is direct. Your request is sent via the networks of the Internet to the place that holds the information you want to view and it is sent back.

Because of this directness, our Internet service providers (ISPs) know our names, addresses, search histories and the sites that we are visiting. It is also how the websites we view know our unique Internet Protocol (IP) address. It is because of this direct connection that companies such as Amazon know everything we view and even how long we've lingered upon a page. Law enforcement agencies are able to capitalize on this directness and can pinpoint who posted what information on an online chat forum.

Tor accesses information on the Web in much the same way, but it breaks up the direct connection. After a fashion, the Tor browser is a bit like an anonymous version of the children's game of telephone. You send your request for a particular video or bit of information to a computer somewhere in the Tor network. This computer then relays that information on to another computer somewhere else in the network. Once again, this computer simply relays your request onwards to yet another machine. This third machine in the game of telephone then requests the information you want to view and sends it back to you along a similar, disjointed path.

Breaking up the request in this way means that different people can see different parts of what you are viewing online, but it is exceptionally difficult, although not impossible, for any one person to connect all the dots to pinpoint who you actually are (Owen and Savage 2015). Your ISP, for example, which normally knows exactly what sites you are visiting, can only see that you are sending a request to the first computer in the network. On the other end of things, the website can tell a lot about the computer that is accessing their content, but this information does not relate to your computer, instead linking to the last of the three computers in the game of telephone. The computers in the relay system know about their neighbour, but no more than that. The first link knows you and the middle computer, but not the end computer or the content viewed. The middle link knows the first computer and the end computer, but not you or the destination of your request. The end computer knows the destination and the middle computer, but not who you are. Layered onto this broken routing of your request is the heavily encrypted signal that prevents data flowing across the Tor network from being accessible to prying eyes.

Tor is not just a way to view online content anonymously. You can also host content, but only in a way that is accessible to other users of the Tor browser. Put another way, you can be the one running the website to which people venture for their bits of information, whatever they might be. The process by which anonymity is obtained is similar to that laid out above. The website itself moves around from server to server in the Tor network. Changes to the website are made using the same three-relay system that is used to prevent the website or server from knowing who is hosting the page. Anonymity is secured.

Finally, it is important to clear up at the outset that, while large parts of the Dark Web are only reachable via Tor, the Tor browser itself can actually be used for other far more innocent purposes, such as simply surfing the day-to-day Web, free from the constraints of censored content and concern over state or corporate surveillance. If you try to download and use Tor (a process that is very easy), you will find that you never need to venture into the seedy underbelly of the Internet if you don't want to. Instead, you can use the Tor browser just like Google Chrome or Mozilla Firefox to check news websites, look at funny memes or anything else you would do normally when browsing the Internet.[4] Even these routine activities are rendered anonymous by Tor.

The end result of this system is a way to use the Internet anonymously, with all the immunity that provides. Clearly, as shown in the next section, that anonymity opens the door to abuses.

THE DARK SIDE OF ONLINE ANONYMITY

The Dark Net certainly is the seedy underbelly of the Internet. Its sordid nature is exemplified in a few stories about drugs, assassination, trolling and child abuse.

In the early years of this decade, a site popped up on the Dark Web called Silk Road. The reference to the ancient trading route from the Orient to Europe was not a mistake. The website was like an illegal version of Amazon, eBay, Kijiji or Craigslist. It aimed to connect sellers of items ranging from drugs to assassinations-for-hire with eager customers with money to burn.

Silk Road started in February 2011. One study observed activity on the website during a six-month period in 2012 and found that Silk Road, while selling all sorts of illegal content, was mostly a proverbial "drugstore." Categorizing all the things that were for sale on the site, the authors found that "the four most popular categories are all linked to drugs," along with 90 percent of the top 10

4 Plug-ins are limited on Tor, so you might not have the full range of functionality you would on another web browser, but the idea that you could just use Tor for your normal Internet activity is valid.

categories and 80 percent of the top 20 (Christin 2012, 8). The transactions were anonymous due to the use of the Tor network and payments were made with a so-called crypto-currency known as bitcoin, which is a purely digital means of payment that leaves no trace.

Silk Road quickly surpassed other illegal market sites, with its revenue and traffic expanding rapidly. In an uncomfortable mix of metaphors, the site was owned by a then 29-year-old man who went by the moniker Dread Pirate Roberts — taken straight out of the 1980s movie *The Princess Bride*. By 2012, the site operators were earning upwards of $92,000[5] per month, as people were flocking to the site to buy and sell items on the illegal market. The audacity of Silk Road's illegal activities lead US Senator Charles Schumer to call for the site to be shut down in June 2011, noting that it is "more brazen that anything else by light-years" (cited in Koebler 2012).

The investigation into Silk Road started in 2011, when an informant broke word of activity on the illegal marketplace site to personnel at the Department of Homeland Security (DHS). Operation "Marco Polo," as the investigation came to be called, quickly expanded to encompass personnel from the Federal Bureau of Investigation (FBI), DHS, Drug Enforcement Administration, Internal Revenue Service and others (Zetter 2013).

As the law enforcement net was closing in on the Dread Pirate Roberts, the modern-day bandit got desperate, even offering $80,000 to an undercover agent to assassinate a former site administrator that had been captured by the police and turned state's evidence. The police staged the killing of the site administrator just to draw the noose that much tighter around Dread Pirate Roberts' neck (ibid.). Ross Ulbricht, the Dread Pirate Roberts, was arrested in October 2013 and the site was taken down. It was a clear victory.

It was also very short lived. Silk Road 2.0 popped up on the Dark Net in November 2013, just one month after the arrest of Ulbricht. Again, the website expanded rapidly, quickly having as many as 150,000 active users and processing, according to FBI records, as much as $8 million in monthly sales (Cook 2014). Within a year, this new incarnation of the illegal marketplace was taken down and Blake Benthall, the Silk Road 2.0 site administrator and former Space-X employee, was arrested.

Another win, another drop in the pond. Silk Road 3.0 was online within a few hours of Benthall's arrest (Knibbs 2014). The cycle goes on, like a globe-spanning game of whack-a-mole.

The dark recesses of the Dark Web are also populated with proverbial trolls, some of whom use Tor to maintain their anonymity, some of whom do not. We have all come across Internet trolls. They surf the Web, posting inflammatory comments, aiming for nothing more than to wreck someone's day, often just for the fun of it.

Consider this telling story of trolling and a needlessly ruined life on the 4chan /b/ board (Bartlett 2014, 13–19).[6] A young university student named Sarah ventured half-naked via a posted photograph into the chat board filled with Dark Web trolls. Her first photo spawned a number of requests for further nudity, which she willingly provided. The requests built gradually to a terrible point. One request asked her to pose naked with her name written on her body. She did it. Another request asked her to pose naked with any medications that she might be taking. She did that, too.

From there, the situation got really ugly. Her mistake was providing the trolls of the Dark Web with enough information to identify her. They found her school, accessed its directory and got her full name, address, phone number and other contact information. Facebook searches revealed her social media profile. From there, the anonymous chatters of the /b/ chatroom then began a "doxing"[7] campaign to wreck her reputation by sharing her naked photos with everyone she had even a slight connection with. Why? Because they could. The viciousness of it all needs to be recounted verbatim to be believed:

> Anonymous: "she gave her first name, her physician's full name, and even the dormitory area she lives in[.] [S]he wants to be found" (Bartlett 2014, 15).
>
> Anonymous: "here is a list of all her Facebook friends. You can message friends, and all their own friends, so that anyone with a slight connection to sarah [sic] via friend of friend knows" (ibid., 17-18).

5 All currency in this paper is in US dollars.

6 4chan actually forbids users from posting using Tor or a virtual private network (VPN) to hide their true identities, so this example might seem slightly outside of the scope of the paper. It is, nevertheless, included for a couple of reasons. First, the extent to which the ban on Tor is followed or enforceable is quite unclear, and it is likely that many routinely violate it. Additionally, the nature of the 4chan board itself provides a degree of anonymity to posters, with users actually being told not to use any identifiable information in their profiles. So, even if the operators would (assuming the rule prohibiting Tor is followed) be able to backtrace posts to a particular person if law enforcement requested it, the ability of people to behave badly because of the anonymity of the board is still present.

7 Doxing basically involves taking people's personal information and spreading it as widely as possible.

> Anonymous: "so has somebody started messaging her friends or family or can I begin with it? (ibid., 18).
>
> Anonymous: "[xxxxx] is her Fone [sic] number — confirmed" (ibid.).
>
> Anonymous: "just called her, she is crying. She sounded like a sad[,] sad sobbing whale" (ibid.)
>
> Anonymous: "Is anyone else continually calling?" (ibid.).

The attacks were personal, devastating and brutal. But the anonymous posters of the /b/ 4chan board were also remorseless.

> Anonymous: "If [she] was clever she would have g[ot] t[he] f[***] o[ut][,] she didn[']t, therefore she deserves the consequences" (ibid., 19).
>
> Anonymous: "I don't give a s*** what happens either. Bitch was camwhoring while she had a boyfriend" (ibid., 19).

The torment promised to be long-lived as well. Amid the maelstrom, Sarah had tried to minimize the damage by deleting her social media accounts, such as Facebook, to limit the trolls' access to the people she knew. But, as one troll noted, the Internet's memory is eternal:

> Anonymous: "Eventually once all this settles she will reactivate it [her Facebook account] and she will have her jimmies rustled once more. She will now never know peace from this rustling. And she's going to have one embarrassing f***ing time with her family" (ibid., 16).

It is sad to see even one life wrecked by a couple of bad choices that are then magnified by the destructive behaviour of anonymous trolls. But this case is in no way an isolated incident. One study found that upwards of two-thirds of people between the ages of 13 and 22 have been bullied online (Butterly 2013). And while certainly not all bullying goes on in the Dark Web — Facebook being a key vehicle of bullying — some of the most egregious often does. It is widespread, malicious and at times enabled by anonymity-granting tools like Tor. Its consequences are both individually and socially destructive.

With its illegal drug and weapon markets and online trolls, the Dark Web seems immoral and unscrupulous, but the scary part is that the shadows of the Dark Web can actually get even darker. Nothing makes that point more clearly than the prevalence of child abuse imagery on the Dark Net.

In 2011, Europol, coordinating with 13 national governments, launched Operation Rescue. The concerted law enforcement action uncovered 670 suspects and led to 184 arrests on child abuse imagery-related charges (Europol 2011). In July 2014, the UK's National Crime Agency arrested some 650 people on various child abuse charges, ranging from the possession of images to the actual abuse of minors (BBC 2014a). In 2015, another 50 suspects were identified in Northern Ireland and 37 charges were laid (BBC 2015). These are just a few examples of the successful instances of law enforcement uncovering pedophilia rings in the recesses of the Dark Web.

Unfortunately, as Gareth Owen and Nick Savage (2015) point out in their study for the Global Commission on Internet Governance, the problem of child abuse images on the Dark Web is probably even more widespread than the record of arrests would lead us to believe. In their innovative study, Owen and Savage actually volunteered a couple of servers to host the Tor network at their university in Portsmouth, United Kingdom. Over a period of several months, they categorized the type of websites found on the Tor-hosted Dark Web. They found that the available sites ranged from whistle-blower chatrooms to pornography sites, illegal markets and child abuse sites. This last category accounted for only a small fraction of all sites hosted on the Dark Web. Unfortunately, they also found that over 80 percent of the actual traffic along the Tor anonymity network went to this small proportion of sites (ibid.).

The lesson from all this is that anonymity allows the Dark Web to be a very nasty place indeed, and Tor makes this type of behaviour possible. Illegal markets selling drugs and guns to whomever will pay, malicious trolls and those who want to harm children, are but a few of the villainous activities going on within the lower recesses of the Internet.

The Virtuous Protection of the Shadows

But the anonymity of the technology of Tor cuts both ways — while people can use the network for villainous purposes, people can also use it for good.

Anonymity is important for the possibility of democracy. Anonymity provides space for people to think and voice opinions that are against the grain. Anonymity ensures both protection for an individual that holds a minority point of view and a window of opportunity for the majority consensus to be challenged by outside ways of thinking. As noted in a US Supreme court decision, *McIntyre v. Ohio Elections Commission*, "Anonymity is a shield from the tyranny of the majority….It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation…at the hand of an intolerant society" (cited in Electronic Frontiers Foundation, n.d.). Without a healthy public debate encompassing all viewpoints, democracy

shrivels. In non-democratic countries, the presence of anonymity is the only way that people can voice contrary points of view against despotic regimes in the hope of securing political freedom.

For its part, the Tor Project website maintains that political activists, reformers, journalists, civil rights workers and development workers can use Tor in repressive countries to circumvent censorship and, to some extent, avoid the prying eyes of state and corporate surveillance. Use of the anonymity network has also been suggested by human rights groups. Reporters Without Borders, for example, recommends the use of Tor as a part of its journalist's "survival kit" (Murray 2014). In its somewhat older report on Internet usage in China, *Race to the Bottom*, Human Rights Watch supported the use of Tor (Human Rights Watch 2006). And the human rights advocacy group, Global Voices, suggests that Tor is useful for dissidents and activists (Global Voices, n.d.).

All of these suggestions for using the Tor network might or might not translate into people actually using it for noble purposes in regimes that mean harm to ordinary citizens. Unlike the high-profile instances of online drug busts and child pornography arrests, which are both on the moral high ground and newsworthy, there are few public stories of political activists using Tor. Repressive regimes do not broadcast when they break the encryption of the network and throw people who are simply asserting their right to free expression into dank prisons. Those who use Tor to avoid surveillance or to circumvent censorship are also not likely to publicly proclaim the specifics of their use of the network (or even that they use it at all), since the whole point of the system is to keep one's online activity anonymous.

There is another way, however, to discover whether people really do use the Tor Dark Web in repressive countries. Rather than have people self-report that they use the network, one can look at usage numbers per country. While many of the specifics are unknowable (as befits an anonymity network), the Tor Project provides data on the number of users of its network per country. Of course, each country has a different number of Internet users and different rates of Internet penetration, so you it isn't just a matter of counting the number of users and saying that the largest number of users are in either repressive or liberal regimes. Instead, to get at whether the level of political rights in a country drives usage of the Tor network, you need to use special statistical methods with a large sample size that can account for other factors that might also lead to people using the network. The process is not as complex as it sounds. At their most basic level, statistical methods can give you an impression of how often a certain level of political rights is associated with either high or low use of the Tor bridge network, given the effect of a host of other factors.

Before turning to the outcome of the statistical tests, it is a good idea to explain how statistical methods can produce some relatively intelligible answers. The basic question explored in another study (Jardine, n.d.) is whether people used Tor more as political repression increased from 2011 to 2013, which gets at the problem of whether the anonymity of the Dark Net can actually provide a cloak to protect those that want to exercise their rights to free speech and freedom of information.

On the one side, the political rights measure used in this study ranges along a scale from one to seven, and is taken from a widely used measure known as the Freedom in the World Index (Freedom House 2015). The index is scored like a game of golf: lower is better. A score of one, in this case, is the best, and a seven is the worst. Liberal democratic countries such as Canada, the United States and the United Kingdom score a one on the political rights index. Highly repressive countries such as Chad and Swaziland score a seven. The rest of the countries of the world are spread between these extremes.

The outcome to be explained is the use of the Tor network in different countries per year, with a specific focus on the use of what are known as bridges. Tor bridges are another name for the relay computers in the game of anonymous telephone. The one distinction is that unlike normal relays, bridges are not listed publicly, which makes them a better tool for people to circumvent censorship and surveillance in repressive regimes.

Since you would expect more people to use Tor (or for that matter anything) in a large population compared to a small one, the numbers for the outcome to be explained are expressed as a rate per 100,000 Internet users per year in a country. A simple example can demonstrate why normalizing the data in this manner is important: in 2013, the United States had 147,207 Tor bridge users, while Canada only had 23,795 users. On the face of it, it seems like Americans use the network a lot more than Canadians — and in one sense they do. But, as a population as a whole, America actually uses the network less. The United States has 55 Tor bridge users per 100,000 Internet users, while Canada has 79 users per 100,000 Internet users. Expressed in these terms, Canadians actually use Tor bridges at a 43.6 percent greater rate than their American cousins. The normalization matters.

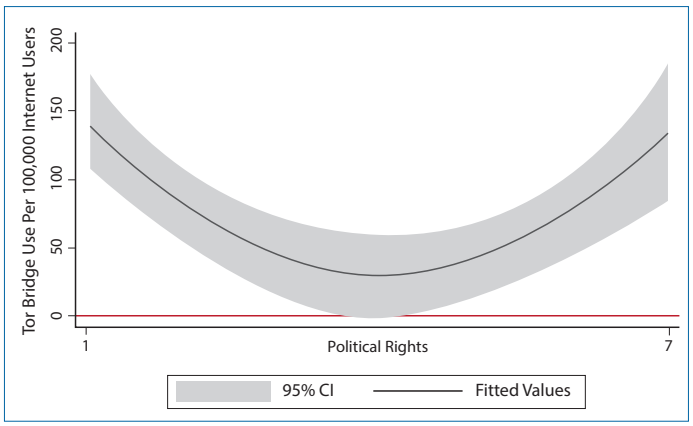
Other factors in addition to political rights also drive use of the Tor network. So, to get a realistic picture of the effect of differing level of political rights, those conditions need to be factored into the equation. Wealth is important to take into consideration because it affects access to information technologies and national bandwidth capabilities. Internet penetration rates are important because someone needs to be able to access the Internet if they are going to actually use Tor. Exposure to foreign ideas and influences also matter, as people need to know about Tor in order to use it

in the first place. Education matters because people need to have a certain level of comfort with information and communications technology in order to use something outside the norm such as Tor. Intellectual property rights regimes matter because they can increase the incentive to use Tor to download illegal movies and songs. The statistical tests include all these factors.[8]

Putting all these numbers to use and running some statistical regressions shows a clear relationship between Tor bridge use per 100,000 Internet users per year and a country's level of political rights. And while political rights do matter, they also *don't* matter in a straightforward way. Rather than use of the Tor network simply increasing as the political rights situation worsens in a country, the relationship between rights and the use of Tor is shaped like a "U." In other words, political rights tend to drive usage rates the most in both highly liberal countries such as Canada and highly illiberal countries such as Swaziland.

The figure below shows how the relationship unfolds across the actual data. As the political rights situation moves from a country such as the United States (political rights = 1) to a country such as Honduras (political rights = 4), political rights tend to drive use of the Tor network less and less. Beyond that low point, a worsening political rights situation starts to drive people toward using the Tor network again, as evidenced by the right hand side of the U-shaped relationship.

Figure 1: Political Rights and Tor Bridge Usage



Source: Jardine (n.d.).

The magnitude of the effect is knowable, too. The table below shows on average just how much a change in the level of political rights in a country matters. Moving from a 1 to a 4 on the political rights scale results in a total reduction of 174.99 users of Tor bridges per 100,000 Internet users per year. Going the other way, from a 5 to a 7 on the political rights scale, leads to a total increase of 68.42 Tor bridge users per 100,000 Internet users per year. In short, political rights matter a fair bit for use of the network.

Table 1: Changing Political Rights and Tor Bridge Use per 100,000 Internet Users per Year

Change in political rights	Change in Tor bridge users per 100,000 Internet users
1 to 2	84.77 less
2 to 3	58.33 less
3 to 4	31.89 less
4 to 5	5.45 less
5 to 6	20.99 more
6 to 7	47.43 more

Source: Jardine (n.d.).

The obvious question at this stage is why do political rights matter in this way? Why form a U-shaped relationship? The reason is that a political regime drives the domestic population's opportunity to use Tor, as well as their need to do so, with the former factor declining as repression increases and the latter rising as political rights decline.

Opportunity, for instance, starts out high in liberal countries, as there are few restrictions on the use of encrypted or anonymous technologies such as Tor. Indeed, a large portion of the Tor Project's funding comes from the US government and the genesis of the program is in US military research labs. As the level of political rights declines, the opportunity to use the anonymity-granting technology worsens, as repressive regimes throw up roadblocks — for example, legislation and technical blocking mechanisms — to prevent people from using the system. China, for instance, has been fairly successful at blocking Tor (MIT Technology Review 2012). Russia, a six on the political rights scale, has offered $110,000 to the person or organization that can crack the encryption and anonymity of the Tor network (BBC 2014b).

Opportunity counts for a lot, so, if it is nearly costless to do so, people will use programs such as Tor for illegal reasons, to circumvent censorship and surveillance by both states and corporations, or simply to support the idea that the anonymous use of the Internet should be something that is valued in society. The result of high opportunity is the high use of anonymity-granting technologies in highly liberal countries.

Need, for its part, is low in liberal countries. People don't have to use Tor in order to do their legal online activity in liberal countries with a strong tradition of rights protection, although the extent to which people should take more steps to be anonymous online, even in liberal regimes, is an open question. As the level of political repression goes up within a country, the need to use anonymity-granting programs like Tor rises.

8 Issues of multicollinearity are discussed in detail in Jardine (n.d.).

This growing need drives people to use Tor in repressive regimes. Here again, the motives vary. Some will do so for illegal purposes. But others will use the network to blow the whistle on corruption, to freely express their political viewpoints, to circumvent censorship and to avoid direct surveillance of their online activity.[9]

The basic point is that repression and the violation of political rights does drive people to use the anonymity network. Oftentimes, people in repressive regimes simply cannot freely express their points of view, circumvent the censorship of important information or avoid the prying eyes of the state without encrypted and anonymous programs such as Tor. Some of what people do online with Tor in repressive regimes will be innocuous and some will even be illicit or illegal, but much of it will be virtuous and aimed at nothing more than exercising some fundamental political rights.

THE POLICY DILEMMA: A DUAL-USE TECHNOLOGY

As demonstrated, Tor is basically a dual-use technology: it can be used for truly awful purposes as well as for good. How it is used matters most, similar to other tools that humanity has invented. We discovered how to harness fire to keep us warm, but then learned that it can be used to ravage and burn. We discovered steel and now use it to make buildings that touch the sky, but before that we learned it can be used to make swords or guns to take lives. The human story is riddled with the invention of technologies that can be used for both good and ill.

Discussions of the use of the Tor network, like discussions of encryption in general, are highly polarized. The one side asserts that the technology needs to be as close to unbreakable as possible so that nefarious actors cannot gain access. A back door into an encrypted system cannot be given only to law enforcement and somehow kept from criminals and political despots. Once an entryway exists, the system is vulnerable. Indeed, purposeful back doors can lead to less privacy, more vulnerabilities as new systems interact with past software and even make governments and service providers tantalizing targets of cybercrime, as they possess the proverbial keys to the kingdom (Abelson et al. 2015).

The other side of the debate asserts that encrypted and anonymous technologies such as Tor hinder law enforcement. FBI Director James B. Comey exemplifies this position. In October 2014, he pointed straight to the other half of the polarization in a speech at the Brookings Institution in Washington, DC:

> Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost? (Comey 2014)

Indeed, at what cost? In one way, the policy issue as it specifically relates to the Tor network boils down to a question about whether the technology does more harm than good. What matters is a net assessment of the impact of the technology. There is no straightforward answer to this question, but the evidence presented here suggests a painful underlying truth — how you frame the parameters of the cost-benefit calculus affects the answer you get.

The uncomfortable reality is that liberal democratic nations that developed and host much of the Tor network are actually having to deal with most of the negative consequences of the system while reaping few of the benefits. The opportunity to use the technology in liberal countries means that Silk Road, trolls and anonymous child abuse websites proliferate, but the gains (dodging the prying eyes of state or corporate content surveillance and circumventing censorship) are fairly minimal. Other, less cumbersome programs (private search engines, such as Duck Duck Go, and VPNs) exist and have roughly the same effect as Tor with more download speed and less potential for abuse, as they retain user data and can cooperate with law enforcement if approached with a valid warrant. Therefore, unless people are engaged in outright illegal activities, the need to use a full-blown anonymity program such as Tor in liberal democratic countries is also limited, because of the presence of constitutional and legal protections of citizen rights, although it is important to not under-represent the extent to which the rapidly evolving nature of the technology of the Internet has outpaced the ability of the legal system to deal with new challenges to citizen's fundamental rights. Based upon the evidence presented above, the idea that Tor provides net benefits to society in liberal democratic countries is unlikely. It most likely does more harm than good.

If the frame of reference is shifted to the net costs or benefits of Tor in a highly repressive country, however, the cost-benefit outcome changes radically. Dissidents, journalists, human rights activists and even ordinary citizens in repressive countries all benefit from the Tor network, even if some of these people might use it for nefarious purposes. In the end, the Tor anonymity network in regimes with low political rights is definitely more beneficial overall.

9 Because Tor has distinct encryption, repressive regimes can often tell when someone is using the program, even if they cannot tell what is being done with the system. Paradoxically, this effort to dodge surveillance of content might put an individual under more scrutiny as the use of encrypted technologies raises red flags in many repressive regimes.

The implicit policy question to come out of this is whether people in liberal countries are willing to pay the cost of the existence of a system such as Tor, given that the benefits are not evenly distributed globally. People in Western countries might decide that the costs are simply not worth it and opt for a state-driven clamp down on the system. This decision would have serious implications for the effectiveness of the Tor network as it functions well in repressive regimes only because most of its infrastructure (computers and servers) reside in liberal countries. Without innumerable volunteered computers around the world, the anonymity of the network would be limited and the ability of Tor to cloak those in need in repressive regimes would be stymied.

WHAT IS TO BE DONE? POLICING

Even if people in liberal countries decide that a program such as Tor is not worth having, the odds of destroying anonymity-granting technologies in general in an era of a global Internet are pretty slim. Tor might be knocked offline, but other programs would simply emerge and take their place. Unless you break the global Internet (which would be excessively expensive in terms of lost GDP), it is simply not possible to prevent people from building technologies that ensure the anonymous use of the Web. In other words, the problem of a dual-use technology like Tor is not likely to go away any time soon. We are stuck with both the good and the bad.

Rather than looking for quick and final fixes (such as destroying Tor outright or altering the technology through back doors in encryption for law enforcement), a more realistic way forward is to focus on actively policing the network.

In the offline world, peace and order are maintained in every segment of society through judicious policing. Socially destructive behaviours are deemed illegal. Crimes are recorded. And criminals are arrested, prosecuted and sent to jail. It is actually ridiculous to think that as more of our daily lives and activities shift online, the online world would not also need to see a rapid expansion of policing efforts to accommodate the shift in our attention and activity.

There has already been some movement in this direction by police forces around the world (Omand, forthcoming). This movement shows that online policing of the Dark Web is in fact possible, expedient and often at least as effective as offline policing.

Despite the use of the Tor network to host the various Silk Road illegal marketplaces, for example, the owners and operators of the sites — as well as many of the largest sellers — were identified and arrested. These arrests show the effectiveness of online policing. The takedown of Silk Road 1.0 is instructive. Police caught the Dread Pirate Roberts through a combination of technological means and the double-edged sword of online anonymity.

Tor is obviously a technically heavy system. And technology played a role in the capture of the server hosting the Silk Road and the ultimate arrest of Ross Ulbricht. In the initial prosecution filing against Ulbricht, the FBI indicated that it found the location of the Silk Road server in Iceland due to a misconfiguration on the illegal market's login page, which allowed investigators to type in "miscellaneous" characters in a CAPTCHA window that returned IP address information.[10] Upon further snooping, the FBI realized that the IP address provided by the login page did not correspond to a known node in the Tor network, and was likely the actual physical address of Silk Road rather than a relay in the system (Greenburg 2014a). Technology is a fickle mistress and it betrayed those that were relying upon it to do harm.

Of course, others doubt whether the characters typed into the CAPTCHA by the FBI were really miscellaneous, charging instead that they were actually lines of code designed to hack the login page by duping it into thinking the entries were actually administrative commands (Greenburg 2014b). Both accounts are plausible. Silk Road 2.0, for example, wasn't vulnerable to the same flaw, suggesting either that Silk Road 1.0 was taken down by a configuration issue or perhaps by a now-patched vulnerability (Brandom 2015). Indeed, Ulbricht's defence during his trial that there was an illegal search due to how the FBI found the Silk Road server fell apart. He was sentenced to more than life in prison (Thielman 2015).

Silk Road 1.0 was also taken down because of the very thing that allowed it to operate in the first place: anonymity. Anonymity, that core feature provided by the Tor browser, doesn't stop law enforcement. Instead, it actually makes law enforcement efforts, in some ways, easier. Buyers or sellers on Silk Road, trolls and child abusers cannot say for sure who they are dealing with in an online world. Anonymity limits attribution, but it cuts both ways. No further evidence is needed than the Dread Pirate Roberts, who offered money to an undercover cop to undertake an assassination of a former site administrator. Child abuse sites are also routinely infiltrated by law enforcement. Police from the United Kingdom and Australia, for example, infiltrated one online child abuse ring of up to 70,000 members "to identify the members who posed the greatest danger to children. Police also sometimes posed as children online as part of the investigation" (NBC News, n.d.).

Online policing is also as expedient as offline policing. The anonymity of Tor does not necessarily slow down law

10 CAPTCHAs are those website windows with blurry letters and numbers that are designed to fool spamming machines, but allow humans to access a site.

enforcement efforts. The fact that the Silk Road networks were taken down, often within a year of their launches, shows the speed at which online policing can work. As a parallel analogue example, Project DISTRESS was launched in Manitoba, Canada, in October 2013, and culminated 15 months later in the arrest of 14 suspects in a major drug trafficking ring (RCMP 2014). The scope of this real-world effort is smaller than Operation Marco Polo to take down Silk Road 1.0, but the timelines are roughly the same. If anything, the online version was a larger endeavour but took less time to complete. Online policing seems to be at least as quick as its analogue cousin.

The fact that new Silk Road marketplaces, trolls or child abuse sites keep popping up in the wake of arrests and shutdowns is also nothing new, and should not be taken as evidence that online policing is not effective. Offline, the arrest of a street-corner drug dealer often leaves a void that is quickly filled by someone else. This doesn't mean that we should stop arresting drug dealers. It means that we are stuck with the problem of people selling drugs, at least until the demand for what is being sold goes away or the arrest and prosecution for such activity is certain. The same logic applies online. Yes, new sites will always pop up as the old ones are taken down and arrests are made, but this just means that governments need to keep policing the network. It is part of the cost of the Internet. To obtain all the benefits that the Internet provides, we need to ensure it is as safe as possible, but we don't want to destroy it completely, which is the only way prevent crime from occurring online.

The call for greater online policing is not the same as saying the state should be allowed to intervene indiscriminately into people lives. Offline, the police cannot go into people's homes whenever they want, but they can patrol the streets and catch people in the act of committing crimes. The same sort of logic should apply online. Police should not be allowed to access the data on a person's computer or their ISP records without a warrant. At the same time, they are allowed to sit in chatrooms to monitor conversations and even pose as potential victims to catch predators. They are also allowed to pose as sellers or buyers on illegal markets to track down people who are actually committing crimes. In short, the new "beat" is shifting from the street to the websites and chatrooms of the Internet. This is the reality of the digital age. Certain tactics remain off limits — and law enforcement should not purposefully take advantage of the presence of legal ambiguity to overreach — but the Internet won't work as a global free-for-all.

This policing should also avoid politicizing the core infrastructure of the Internet. As Samantha Bradshaw and Laura DeNardis (n.d.) note, attempting to police intellectual property rights regimes, for example, through the core infrastructure of the Internet (in their case, the Domain Name System) can lead to unintended consequences that risk damaging or even breaking the network. Instead, policing of the Dark Web should occur largely on top of the infrastructure at the social or content level. Law enforcement officers should have a presence inside an online chatroom frequented by pedophiles, but they should not manipulate the infrastructure that supports the creation of online chatrooms in the first place.

There is a bit of a tension between the legitimate use of technological methods to identify those that are breaking the law and the idea that manipulating core infrastructure should be off limits. The use of technology to fight crime falls along a continuum. At one end are legitimate technical investigations, such as the methods used to take down Silk Road 1.0. This kind of activity is acceptable because it exploited a weakness in a particular site, rather than trying to break the whole system. At the other end, trying to simply knock Tor offline is a more fundamental politicization of the infrastructure of the system, affecting both the good and the bad indiscriminately, and therefore should be disallowed.

At the margin, there is a lot of ambiguity about what is acceptable. The takedown of Silk Road 2.0 points out the blurry line. To identify the users of Silk Road 2.0, the FBI volunteered "reliable IP addresses" to the Tor hidden services network upon which the newest incarnation of the illegal marketplace was based. This allowed the FBI to subtly change the coding so that they could pinpoint the identity of users that had employed their relays to reach the illegal marketplace. The operators of Tor noted this trick after six months, and provided a patch that once again improved the anonymity of Tor. For Silk Road 2.0 and Blake Benthall, it was too late. The FBI had tracked down the server and 78 sellers and buyers (Brandom 2015). Exploiting the voluntarist nature of the Tor infrastructure is right at the line of unacceptable use of core infrastructure for policing. It was an indiscriminate attack on all Tor users, so it probably went a bridge too far. Either way, the Silk Road 2.0 example highlights the tension.

LIMITATIONS TO ONLINE POLICING AND AREAS FOR POLICY INTERVENTION

There are limits to the effectiveness of online policing that concerted policy actions can help to overcome.

One limitation is that online criminals can be global, even while most law enforcement agencies (Interpol excepted) are local. If a criminal is not in the same jurisdiction as the police that identify his or her actions as illegal, policing gets immensely more complicated. The problem is even more pronounced when Tor bounces your signal around the world, effectively involving multiple jurisdictions. In some cases, policies are in place to allow states to cooperate by sharing evidence across borders. Foremost among these

mechanisms are what is known as mutual legal assistance treaties (MLATs).

The problem is the MLAT process is in massive need of reform. Proposals exist for how it should be reformed. One study maintains that MLAT reform must emphasize proportionality, the protection of human rights, transparency, heightened efficiency and scalability if they are to become an effective tool in the international police officer's tool kit (Woods 2015). That would be a good start.

MLAT reform can certainly help to make the process of Internet policing more effective, but it won't solve the root of the problem, as online crime is highly mobile and can drift to countries that are outside of the effective MLAT regime. For MLATs to work, two states need to have an agreement in place and both need to view something as illegal in order for the process to be effective. Cooperation through the MLAT process is quite likely between liberal democratic countries because they share legal principles and political dispositions. Cooperation on cybercrime is less likely between Western countries and nations such as China and Russia, which disagree on so many fundamental issues. Moreover, at the end of the day, MLAT reform might fail as the Internet governance system is becoming increasingly contentious (Bradshaw et al. 2015). This is not a small hurdle, but it is not insurmountable either.

Other specific efforts at international coordination of law enforcement agencies can do nothing but help. Interpol's Global Complex for Innovation is a prime example. It aims to build relationships between police forces, increase various countries' understanding of digital security issues and facilitate capacity building to overcome the fact that many local and national police forces just don't have the resources, training and wherewithal to deal well with cybercrime. More international coordination should help with the trans-border portion of the cybercrime problem.

But coordination failures are not just a problem between nations. Most countries have internal layers of police, ranging from the national to the local. Coordination failures between these levels can often stymie effective efforts at policing cybercrime. Local and national police have both critical resources and deficiencies in the battle against cybercrime. Local police can often be the first to learn of a cybercrime (say, identity theft or cyber harassment), but often lack the capacity and jurisdiction to act effectively.[11] National law enforcement usually has the capacity and jurisdiction to act effectively, but can lack knowledge that a particular cybercrime is occurring.

The strengths and weaknesses of local and national-level law enforcement are complementary. By working together, the knowledge of local police can be paired with the resources and capacity of national law enforcement. Specialization remains efficiency-enhancing here, so local police should not be trying to bust international online fraud rings and national-level law enforcement should not be trying to get local victims to report crimes directly to them (although national-level crime reporting is increasingly effective at scale). Each level should stick to its strengths, but work together in a coordinated way to limit online crime.

Even with greater coordination, more training and capacity are still needed. Local law enforcement, in particular, tends to be undertrained and under-resourced to deal with cybercrime. As Darrel Stephens, executive director of the Major City Chiefs Police Association, noted in 2013, "Most local police do not have the capacity to investigate these cases even if they have jurisdiction" (cited in Sullivan 2013). Stephens is also cognizant of how local police departments will need to adapt, stating further that, "Police will need to become more equipped to deal with cybercrime in the future" (ibid.). And that "most major cities have a limited capability, but more will be required" (ibid.). Many crimes are shifting online, so resources that are otherwise dedicated to policing offline crime could be usefully moved to combat online crime instead. Even with the redistribution of efforts, more resources are needed to effectively combat online crime.

Obtaining more resources at the local level is likely to come with some growing pains. More resources typically follow greater need, but local police face a perverse incentive when it comes to something as foundational to crime fighting as recording that a crime has even occurred. A physical burglary or violent crime in a jurisdiction will faithfully be recorded accurately and quickly in most cases. A cybercrime of harassment or theft is far less likely to be counted. The reason is that it is harder for local police to address these crimes, given resources, capacity and the jurisdiction in which they work. As a result, these crimes are more likely to remain off the books.[12] To include them would inflate the crime rate in an area and probably the unsolved crime rate as well, all of which reflects poorly upon the local police department.

However, by trying to avoid a rising crime rate, local law enforcement is hamstrung in their ability to solicit or collect new resources or capacity over the long term. Heads might roll if the crime rate goes up in the short run, but this could be a window of opportunity for local police departments that need more training and resources to combat cybercrime. In most cases, a growing need (higher crime rates) is matched with more resources. In the long term, the only way to strengthen local police departments to

11 Many countries have national-level information collection agencies, so information about ongoing crimes is not always clustered at the local level. This varies by country and likely by crime type as well.

12 At the 2015 Global Conference on Cyberspace in The Hague, Richard Clayton pointed out that this happens. To the extent that I may have misunderstood his point, the fault is my own.

help them fight cybercrime is to recognize that cybercrime has local victims, even if perpetrators could be anywhere in the world and the jurisdictional lines are blurry.

Increasingly, coordination must also occur between governments and private sector actors. One example of this coordination in action is the recent breakup of a large botnet by European law enforcement and Microsoft (Microsoft News Center 2013). Private companies own and operate much of the software, hardware and networks of the Internet, while law enforcement has the jurisdiction to pursue criminals. Public-private partnerships between law enforcement and private companies will likely be the way of the future. When done well, public-private collaboration can be a massive force multiplier, leading to the more effective policing of the Dark Web.

Policing anonymity-granting technologies is also challenging because the system is decentralized, based upon volunteered servers and does not retain data. The messaging application Wickr is an analogous example. They will readily comply with warrants that require access to their servers; however, since they do not retain any data generated by the users of their service, law enforcement cannot find any useful information by searching the system. Tor is similar in that it does not retain data. Additionally, the volunteered nature of the network means that even if someone were logging traffic through Tor relays (which the system is not designed to do), law enforcement in any one country would be hard pressed to find this data. Changing the legal rules so that companies and organizations such as Tor would be required to retain data for a period of time — for instance, six months — would be one way to allow for semi-anonymous communications, but ensure that when law enforcement is cued to a potential crime, they can get access to what they need. The big problem with this approach is how it would be applied in repressive regimes. In those countries, even a six-month retention of data can lead to imprisonment for activists, journalists and human rights workers. As a result, those behind Tor would never accept a mandated retention period of data.

A final limitation is that cybercrime is rapidly increasing, which threatens to overwhelm any and all available policing capacity of nations. Cybercrime is certainly going up, but it is not as bad as we commonly think it is. The key reason is that cyberspace is actually growing as fast, and sometimes faster, as the growth in new vulnerabilities, web-based attacks and the costs of cybercrime. In other words, the rate of crime is not as bad as the picture often portrayed in the media and is, in some cases at least, even improving (Jardine 2015). In other words, law enforcement still has a reasonable chance, and is doing a fairly good job, of holding web-based crime at bay. Policing the Dark Web can be successful.

CONCLUSION

Overall, Internet policing is maybe not ideal. It would be better if people just stopped using anonymity networks such as Tor to do illegal things. That would allow the network to be used to circumvent censorship and surveillance in repressive countries without any of the socially damaging spillover that online anonymity produces.

The network is fragile, despite its resilience, and if we try to find a quick and easy technological fix to problems that are actually social, we run the very real risk of breaking the Internet. Rather than discarding Tor or breaking the anonymity and encryption of the system through back doors for law enforcement, the focus should instead be on policing what goes on upon the network itself. Policing has the advantage of minimizing the costs that the Dark Web imposes on society, while allowing the Dark Web to have the maximum potential positive effect globally. It is not perfect, but it is the best we can probably do.

Acknowledgements

This paper has benefitted from the eyes of, in no particular order, Secretary Michael Chertoff, Laura DeNardis, Bill Graham, Gordon Smith, Pindar Wong and Leanna Ireland. It has also been polished by Carol Bonnett and Vivian Moser. Despite the collective wisdom of all these eyes, problems might linger. These are my errors alone.

WORKS CITED

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter and Daniel J. Weitzner. 2015. *Keys Under the Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications.* Computer Science and Artificial Intelligence Laboratory Technical Report. http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

Bartlett, Jamie. 2014. *The Dark Net: Inside the Digital Underworld*. London, UK: William Heinemann.

BBC. 2014a. "Child abuse image investigation leads to 660 arrests." BBC News, July 16. www.bbc.com/news/uk-28326128.

———. 2014b. "Russia Offers $110,000 to Crack Tor anonymous Network." BBC News, July 28. www.bbc.com/news/technology-28526021.

———. 2015. "50 arrests in NI online abuse images probe in past year, say police." BBC News, March 15. www.bbc.com/news/uk-northern-ireland-31896685.

Bradshaw, Sam and Laura DeNardis. n.d. "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Universality, and Freedom." Unpublished manuscript.

Bradshaw, Sam, Laura DeNardis, Fen Hampson, Eric Jardine and Mark Raymond. 2015. "The Emergence of Contention in Global Internet Governance." Global Commission on Internet Governance Paper Series No. 17. https://ourinternet-files.s3.amazonaws.com/publications/no17.pdf.

Brandom, Russel. 2015. "Feds found Silk Road 2 servers after a six-month attack on Tor." The Verge, January 21. www.theverge.com/2015/1/21/7867471/fbi-found-silk-road-2-tor-anonymity-hack.

Butterly, Amelia. 2013. "'Growing trend' of cyberbullying on social networks." BBC News, October 2. www.bbc.co.uk/newsbeat/article/24364361/growing-trend-of-cyberbullying-on-social-networks.

Chertoff, Michael and Tobby Simon. 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security." Global Commission on Internet Governance Paper Series No. 6. https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf.

Christin, Nicolas. 2012. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." Working paper, November 30. http://arxiv.org/pdf/1207.7139.pdf.

Comey, James. C. 2014. "Speeches." www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Cook, James. 2014. "FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0." Business Insider, November 6. www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11.

Electronic Frontiers Foundation. n.d. "Anonymity." www.eff.org/issues/anonymity.

Europol. 2011. "Operation Rescue." www.europol.europa.eu/content/operation-rescue.

Freedom House. 2015. "Freedom in the World: Aggregate and Subcategory Scores." https://freedomhouse.org/report/freedom-world-aggregate-and-subcategory-scores#.Va6gr_lVhBc.

Global Voices. n.d. "Anonymous Blogging with WordPress & Tor – ARCHIVED." Global Voices.

Greenburg, Andy. 2014a. "The FBI Finally Says How It 'Legally' Pinpointed Silk Road's Server." Wired, September 5. www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/.

———. 2014b. "FBI's Story of Finding Silk Road's Server Sounds a Lot Like Hacking." Wired, September 8. www.wired.com/2014/09/fbi-silk-road-hacking-question/.

Human Rights Watch. 2006. *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship*. Human Rights Watch. www.hrw.org/reports/2006/china0806/china0806webwcover.pdf.

Jardine, E. n.d. "Tor, What is it Good For? Political Rights and the Use of Anonymity-Granting Technologies." Unpublished paper.

———. 2015. "Global Cyberspace is Safer than You Think: Real Trends in Cyberspace." Global Commission on Internet Governance Paper Series No. 16. https://ourinternet-files.s3.amazonaws.com/publications/no-16_Web.pdf.

Knibbs, Kate. 2014. "Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs." Gizmodo, November 7. http://gizmodo.com/silk-road-3-is-already-up-but-its-not-the-future-of-da-1655512490.

Koebler, Jason. 2012. "Online Black Market Drug Haven Sees Growth Double." *U.S. News*, August 7. www.usnews.com/news/articles/2012/08/07/online-black-market-drug-haven-sees-growth-double.

Microsoft News Center. 2013. "Microsoft, the FBI, Europol and Industry Partners Disrupt the Notorious ZerAccess Botnet." December 5. https://news.microsoft.com/2013/12/05/microsoft-the-fbi-europol-and-industry-partners-disrupt-the-notorious-zeroaccess-botnet/.

MIT Technology Review. 2012. "How China Blocks the Tor Anonymity Network." April 4. www.technologyreview.com/view/427413/how-china-blocks-the-tor-anonymity-network/.

Murray, Andrew. 2014. "The dark web is not just for paedophiles, drug dealers and terrorists." *The Independent*, August 18. www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html.

NBC News. n.d. "Massive Online Pedophile Ring Busted by Cops." www.nbcnews.com/id/42108748/ns/us_news-crime_and_courts/t/massive-online-pedophile-ring-busted-cops/#.VcirBPlVhBc.

Omand, David. forthcoming. "The Dark Net: Policing the Internet's Underworld." *World Policy Journal.*

Owen, Gareth and Nick Savage. 2015. *The Tor Dark Net*. Global Commission for Internet Governance Paper Series No. 20.

RCMP. 2014. "Project DISTRESS." www.rcmp-grc.gc.ca/mb/news-nouvelles/2014/project-projet-distress-20141211-eng.htm.

Sullivan, Eileen. 2013. "Local Police Get Into Cybercrime Fighting Business." *Huffington Post Tech*, April 13. www.huffingtonpost.com/2013/04/13/police-cybercrime_n_3075427.html.

Thielman, Sam. 2015. "Silk Road operator Ross Ulbricht sentenced to life in prison." *The Guardian*, May 29. www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced.

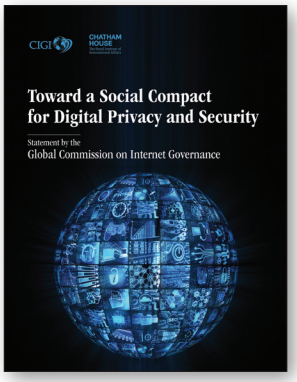
Woods, Andrew. 2015. *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*. Global Network Initiative. January. https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

Zetter, Kim. 2013. "How the Feds Took Down the Silk Road Drug Wonderland." *Wired*, November 18. www.wired.com/2013/11/silk-road/.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem. Launched by two independent global think tanks, the Centre for International Governance Innovation and Chatham House, the GCIG will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

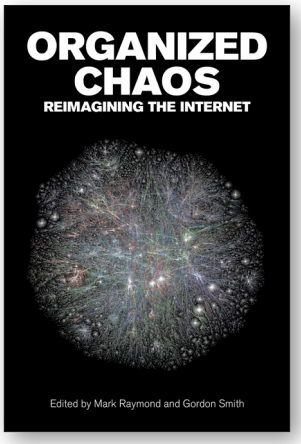


Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance

On the occasion of the April 2015 Global Conference on Cyberspace meeting in The Hague, the Global Commission on Internet Governance calls on the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet. It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet. This statement provides the Commission's view of the issues at stake and describes in greater detail the core elements that are essential to achieving a social compact for digital privacy and security.

Available for free download at www.cigionline.org/publications



Organized Chaos

CDN$25

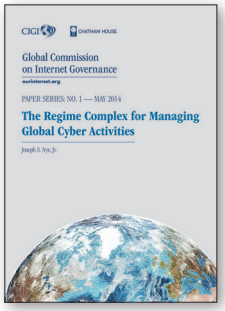
Edited by Mark Raymond and Gordon Smith

Anonymous. Cybercrime. Hacktivist. Cyber security. Now part of the lexicon of our daily language, these words were unknown a decade ago. The evolution and expansion of the Internet has transformed communication, business and politics, and the Internet has become a powerful influence on everyday life globally. But the Internet is a medium that is not controlled by one centralized system, and the debate over who will govern the Internet has commanded attention from a wide range of actors, including states, policy makers and those beyond the traditional tech industries.

Organized Chaos: Reimagining the Internet examines the contemporary international politics of Internet governance problems, exploring issues such as cybercrime, activities of the global hacktivist network Anonymous and "swing states," and highlighting central trends that will play a role in shaping a universal policy to govern the Internet. In this book, some of the world's foremost Internet governance scholars consider the critical problems facing efforts to update and refine Internet governance at an international level and the appropriate framework for doing so. This volume provides the basis for developing a high-level strategic vision required to successfully navigate a multi-faceted, shifting and uncertain governance environment.

Available for purchase at www.cigionline.org/bookstore

GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES



The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations
GCIG Paper Series No. 10
Michael Chertoff and Paul Rosenzweig

Connected Choices: How the Internet is Challenging Sovereign Decisions
GCIG Paper Series No. 11
Melissa E. Hathaway

Solving the International Internet Policy Coordination Problem
GCIG Paper Series No. 12
Nick Ashton-Hart

Net Neutrality: Reflections on the Current Debate
GCIG Paper Series No. 13
Pablo Bello and Juan Jung

Addressing the Impact of Data Location Regulation in Financial Services
GCIG Paper Series No. 14
James M. Kaplan and Kayvaun Rowshankish

Cyber Security and Cyber Resilience in East Africa
GCIG Paper Series No. 15
Iginio Gagliardone and Nanjira Sambuli

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime
GCIG Paper Series No. 16
Eric Jardine

The Emergence of Contention in Global Internet Governance
GCIG Paper Series No. 17
Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?
GCIG Paper Series No. 18
Ben Scott, Stefan Heumann and Jan-Peter Kleinhans

The Strengths and Weaknesses of the "Brazilian Internet Bill of Rights": Examining a Human Rights Framework for the Internet
GCIG Paper Series No. 19
Carolina Rossini, Francisco Brito Cruz, Danilo Doneda

The Tor Dark Net
GCIG Paper Series No. 20
Gareth Owen and Nick Savage

Available for free download at www.cigionline.org/publications

CIGI
Centre for International Governance Innovation
www.cigionline.org

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

Communications

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org