Original Manuscript

new media & society
1–20

DOI: 10.1177/1461444817733134
journals.sagepub.com/home/nms
SAGE

Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies

Eric Jardine
Virginia Tech, USA

Abstract
Do heightened privacy perceptions, censorship concerns and exposure to online crime affect people's level of opposition to dual-use technologies such as the Dark Web? If they do, then how much do these factors actually drive baseline levels of opposition to the Dark Web? Do privacy and censorship concerns get amplified in regimes with significant Internet restrictions? Does Internet freedom itself affect people's baseline levels of opposition to Tor and other Dark Web technologies? Using new survey data on 17,121 Internet users in 17 different countries, a series of mixed-effect order logit regressions reveal that privacy and censorship concerns are both significant predictors of less opposition to the Dark Web. Past exposure to online crime, in contrast, significantly increases opposition to the Dark Web. Interestingly, restrictions on Internet freedom do not amplify privacy and censorship concerns, but Internet freedom itself is related to baseline levels of opposition to the Dark Web forming an inverted-U-shaped pattern.

Keywords
Censorship, Dark Web, Darknet, data breaches, Internet Freedom, privacy, survey

Introduction

Dark Web technologies have many uses.[1] Since their inception in US naval research labs, Dark Web technologies have quickly become an indispensable tool for those who need

Corresponding author:
Eric Jardine, Virginia Tech, 220 Stanger Street, Blacksburg, VA 24061, USA.
Email: ejardine@vt.edu

to hide what they are doing online. In some cases, people hide behaviour that is illicit, immoral or outright illegal. Only 1 month after a Darknet child abuse imagery site named Playpen was launched in August 2014, for example, it reportedly had over 60,000 members. By 2015, the membership roll had increased to almost 215,000 people. Before being taken offline by the Federal Bureau of Investigation (FBI), Playpen was reportedly receiving some 11,000 unique visitors each week and contained over 117,000 posts (Cox, 2015).

Illegal marketplaces selling drugs, guns and all sorts of illicit material also pop up on the Dark Web with troubling regularity so as to mask the conduct of criminal commerce. Markets, such as the now shutdown Silk Road or Evolution, sell drugs to any who dare brave the perilous underworld of the Internet. Usage of these online illegal marketplaces continues to increase, with one global survey of over 100,000 Internet users finding that the nearly 10% of people purchasing narcotics had done so on the Darknet, and that fully only 5% of respondents actually indicated that they did not purchase or use drugs before buying them online (Global Drug Survey, 2016). Clearly, whether the end is the dissemination of child abuse imagery or the purchase of illegal drugs and services, Dark Web technologies can provide cover for those who are up to no good.

Yet, in another context, ordinary people can use anonymity-granting technologies to protect their privacy from government agencies, political opponents, trolls, data-hungry corporations and even Internet service providers. People in highly repressive regimes can also turn to anonymity-granting Dark Web technologies, such as the Tor Browser, to circumvent censorship, exercise a right to free expression and maintain their privacy in the face of an abusive regime (or even non-governmental vigilantes, trolls or bullies). Human Rights Watch (2006), for instance, advises that people use Tor in China to avoid the abuses of the state, although recent crackdowns on the technology make doing so more difficult. Global Voices, a curator and publisher of Internet-based media of various stripes, suggests that those who wish to blog anonymously should use Tor. And, in a similar vein, Reporters Without Borders advises that journalists use Tor to protect themselves as they report on abuses from around the world (Tor Project, n.d.).

From a policy perspective, the various uses to which Dark Web technologies can be put generate a ‘Dark Web Dilemma’, where there is no good policy response to the technology (Jardine, 2015). On one hand, efforts to shut down the network can harm those people in repressive regimes that truly rely upon it for protection, while, on the other, keeping it up causes harm to those who are either directly or indirectly affected by masked online criminal behaviour.

Yet, in a world of seemingly endless terrorist threats, online abuses and proliferating cyberattacks, many policymakers, particularly those in law enforcement agencies, have increasingly begun to agitate for policies that would restrict technologies that prevent lawful access to the online activities of users. For example, sensationalist media accounts of how Darknet markets played a role in supplying weapons to the gunmen in the November 2015 attacks in Paris (Jenning et al., 2015) and other such similar events are often all that is needed for policymakers to advocate for ‘back doors’ in encryption and a more general restriction on Dark Web technologies that in combination hide users from prying government eyes.

Public opinion often has a substantial effect on public policy, particularly when the issue at hand is highly salient for the general population (Burstein, 2003). As a result, political machinations aimed at tamping down technologies that protect potentially malicious actors can be readily bolstered, or even amplified, by outpourings of public support. Globally, the Internet using public does tend to be fairly strongly opposed to Dark Web technologies, which further strengthens the hand of those political forces aiming to shutter the anonymous portions of the Internet.

In 2016, for example, the Centre for International Governance Innovation (CIGI) released a survey (the CIGI/Ipsos Global Survey on Internet Security and Trust, 2016), showing that a vast majority, 72% of Internet users across 24 countries, opposed the 'Dark Net' and wanted to shut it down.[2] The polling results were quickly picked up by international media outlets, with 18 high-profile stories appearing in venues such as Reuters (Sharpe, 2016), Wired (Greenberg, 2016), Forbes (Tracy, 2016), The Washington Post (Viebeck, 2016), SC Magazine (Barth, 2016) and numerous others. While establishing a link between public opinion and public policy development is always tenuous, the negative narrative of the initial poll results, amplified by extensive media coverage, plausibly feeds into ongoing debates in the United States, the United Kingdom and elsewhere about limiting the use and functionality of technologies that prevent law enforcement access to user data and identity, including Dark Web technologies such as Tor.

However, top-level results such as those found in the CIGI/Ipsos survey can mask important differences among individual users and fail to identify those factors that might push people into opposing Dark Web technologies. The mechanisms that drive people to oppose Dark Web technologies, therefore, remain unclear. Do individual-level privacy perceptions and censorship concerns matter? Does exposure to online crime make people hostile to the Dark Web? If these individual-level factors do matter, then by how much? What is more, do these factors matter more in countries with higher levels of restrictions on Internet freedom, as might be expected? Moreover, does Internet freedom itself condition people's baseline level of opposition to dual-use technologies like the Dark Web?

In this article, I use respondent-level data from the CIGI/Ipsos (2016) survey of over 17,121 Internet users in 17 different countries, including major Internet centres, such as China, India, Brazil, Germany, the United Kingdom, Turkey, South Africa and the United States, to provide an answer to these questions. The data are weighted to be representative of Internet users in these countries and provide a rich picture of the role of privacy perceptions, censorship fears, concern over online crime and structural-level network freedom as they relate to opposition to Dark Web technologies. In particular, I show that growing privacy concerns tend to lead to a drop of 34.82 percentage points in terms of the predicted probability that someone will oppose the Dark Web. More intensive censorship concerns, in turn, are associated with a decrease of 10.78 percentage points in opposition to the Dark Web. Interestingly, and contrary to expectations, privacy perceptions are amplified by country-level network freedom, not Internet restrictions. Past exposure to data breaches and online crime, for its part, is positively associated with an increase in the predicted probability of opposition to the Dark Web of some 3.03 percentage points.

Freedom on the net – measured at the country level – is not a significant determinant of opposition to Dark Web technology. While the result is not statistically significant, the

pattern of the relationship between network freedom and opposition to Dark Web technologies forms an inverted-U. This result is broadly in line with other empirical findings about the relationship between political rights and actual usage of the Tor network (Jardine, 2016b). The statistical models also show that individual-level gender, sector of employment, education levels and marital status are also significant correlates of opposition to Dark Web technologies.

By way of a roadmap of what is to come, the first section outlines the general contours of the Dark Web, showing how the technology can be used to enable privacy, circumvent censorship, facilitate crime and how the political context might matter. This section also derives empirically testable hypotheses from the potential uses of Dark Web technologies. The second section describes the cross-national survey data used in this study, and specifies the weights used and the structure of the dependent and independent variables of interest. The third section presents the results of a number of mixed-effects logit regressions, which control for country-level effects and isolate for the effect of privacy perceptions, censorship fears, exposure to online crime and country-level rates of Internet freedom. The final section concludes.

The contours of the Dark Web

The Dark Web – or more appropriately Dark Webs as there is no single variant – is anonymized and dark for a reason. The aim of these networks is to hide what people are doing online, so any estimation of how Dark Web technologies are used is inherently speculative. It is always possible that, like the ancient parable of four blind men feeling different parts of an elephant, only to describe the mammoth beast in rather particular and yet incomplete terms, what we know of the contours of the Dark Web might be a non-random slice that gives us some false impressions. With appropriate caveats about generalization aside, what we think we know of the uses and abuses of Dark Web technologies so far paints a mixed picture of banality, illegality and righteousness.

While there are many different entry points into the various parts of the Dark Web, the most common route, by far, is known as The Onion Router or Tor for short. The following discussion derives hypotheses from the uses and abuses of the Tor network, as it is the most popular entry point into the Dark Web. Plausibly, these uses and abuses would be similar in other platforms such as I2P, Freenet and Zeronet. The results, therefore, are potentially broadly indicative of public attitudes towards Dark Web technologies in general.

For users, Tor really has two components. One component is a browser bundle that users can employ to surf the Internet anonymously. The browser takes advantage of a network of volunteered computers all over the world. It anonymizes a person's web activity by encrypting and then bouncing (relaying) a person's web query through at least three randomly selected computers. The other component of Tor is the ability to host unindexed websites on the Darknet. These hidden services appear on .onion urls, as opposed to the more familiar .com or .ca. Tor's browser can be used either to access the surface web anonymously or to access Darknet websites hosted throughout the overlay network. The unindex Darknet .onion urls, on the other hand, can only be administered and accessed by specially configured browsers.

In 2016, the Tor network had, on average, about 2 million daily users. These users are not necessarily 2 million unique individuals, as those who connect to a Tor node, disconnect and then connect again would be counted as two distinct users. Additionally, Tor's 2 million daily users are certainly not evenly divided in terms of how they actually use Tor's Dark Web technology. Most people, for example, use the Tor browser to remain on what is nominally known as the surface web, populated by normal websites such as YouTube, Amazon.com and CNN news. Indeed, reportedly 96.6% of those using the Tor network do not use hidden services and simply go to the surface web (Tor Project, 2015). This behaviour keeps most Tor users well away from any Darknet sites as they are typically understood. It is certainly more than possible to get into trouble on the surface web, but it is also fairly likely that most people are using Tor to access legal and licit services with technological protections that help to ensure their privacy and anonymity rather than attempting to undertake outright illegal activity.

The effect of Edward Snowden's revelations on Tor usage rates highlights the privacy-enhancing value potentially provided by Tor and similar Dark Web technologies (Hampson and Jardine, 2016: 87–88). Tor's monthly usage rate, for instance, grew considerably in the year after Snowden's disclosures about National Security Agency (NSA) surveillance made front page news in June 2013. Certainly, the huge initial bounce in users was not simply due to privacy-concerned individuals flocking to Dark Web technologies. Instead, much of the most pronounced spike was actually caused by increased botnet activity (Higgins, 2013). But as that malicious activity declined and the artificially high rate of Tor usage fell, monthly average usage rates in the years following Snowden remained much higher than before the NSA's snooping tools became public knowledge. Now, something on the order of some 60 million users employ Tor each month as of 2016.

The clear potential to use the Tor network as a privacy-enhancing tool in the face of governments, Internet companies and Internet service providers suggests a first empirically testable hypothesis:

> *H1*. Higher individual-level privacy concerns should be negatively correlated with opposition to the Dark Web.

A related expectation would be that since privacy is most tenuous in repressive regimes, privacy perceptions should matter the most in places where Internet freedom is most severely curtailed. Again, this notion can be empirically tested in the following way:

> *H2*. Privacy perceptions should be most strongly related with less opposition to the Dark Web in regimes with low levels of Internet freedom.

Tor is also an effective censorship circumvention tool. Users in jurisdictions that restrict social media sites, for example, can often find a ready alternative on the Darknet. Sometimes, these social networking sites are specific to the Dark Web and have their own set of norms and online mores (Gehl, 2016). At the same time, however, the major players in the social networking space have begun hosting .onion variants of their

services. Facebook, for example, launched a Darknet version of its popular social media application in 2014. As Runa Sandvik – who is credited with helping Facebook take the Darknet plunge – puts it, the aim of the move is to provide users with added security and help them 'get around the censorship and local adversarial surveillance' (cited in Greenberg, 2014).

Indeed, many people do use systems like Tor to avoid censorship restrictions and reach social networking sites. Since its inception in 2014, Facebook's popularity on the Darknet has consistently grown over time. In June of 2015, roughly a year after it was launched, the number of people accessing Facebook via the Tor network in a given month had increased to 525,000 people. By April of 2016, the number had increased further still finally crack the 1-million-person per month mark (Muffett, 2016). People potentially subverting Internet restrictions to access Facebook, therefore, accounts for around 1.7% of all monthly Tor traffic. This discussion suggests a second hypothesis:

H3. Higher individual-level censorship concerns should be negatively correlated with opposition to the Dark Web.

Like with privacy, repressive regimes that curtail Internet freedom should plausibly accentuate the effect that censorship concerns have upon user opposition to the Dark Web. People can use Tor, for example, to bypass geo-IP restrictions and to view content that is otherwise prohibited within a country due to reasons as variable as copyright, illegality or religious and political proscriptions. The censorship circumvention applications of Dark Web technologies such as Tor are why regimes like China have taken such significant steps to prevent people from even being able to access the technology from within the mainland, although 'Tor bridges' provide a ready alternative access point for users in China. This suggests a fourth hypothesis:

H4. Increasing censorship concerns should be most strongly associated with less opposition to the Dark Web in regimes with low levels of Internet freedom.

Of course, not all of the traffic on the Dark Web is directed towards legal and benign services like Facebook. While users who employ systems like Tor to surf the surface web likely do so to remain private, access geographically restricted content or some combination of both, things get considerably more complicated when anonymous web browsing and anonymously hosted and administered websites are paired together (Moore and Rid, 2016). This mixture is ripe for criminal misdeeds, as neither the user nor the site administrators can be easily identified, tracked or located.

Despite common misconceptions that the summed total of the various Dark Webs is multiple times larger than the surface web, the actual number of Tor-hosted Darknet sites is fairly modest. Estimates on the sheer number of Tor-hosted Darknet sites vary. On the low end, previous research efforts have uncovered around 30,000 active .onion urls at any one point and time (Intelliagg, 2016; Tor Project, 2015). Another study looking at Tor hidden services for a 6-month period found more than 45,000 .onion urls (Owen and Savage, 2015). Clearly, no matter the final number, the Darknet of anonymously hosted

.onion urls is truly miniscule when compared to the hundreds of millions of sites that are active on the surface web.

The often criminal nature of Darknet sites clusters in pretty routine ways across various measurement exercises. In 2013, one look at over 8000 .onion addresses, for instance, found that pornography (17%) and drugs (15%) made up a significant plurality of sites (Biryukov et.al., 2013: 3). In 2016, Daniel Moore and Thomas Rid categorized the content of 5205 sites. Like past work, they found that around 15.5% of all active sites were related to drugs. They also found that 5% of sites were dedicated to violent extremism, 3.5% were dedicated to hacking services and 1.5% of sites were dedicated to the purchase and sale of arms. Once again in a similar vein, Gareth Owen and Nick Savage (2015) also found that 15% of the .onion urls which they observed over a 6-month period were dedicated to drugs.

While drug sites tend, with a high degree of consistency, to be among the most common Darknet sites, the overall pattern of site visits to Tor-hosted .onion urls tells a different story entirely. Owen and Savage's (2015) study is indicative. When categorizing Tor hidden services' urls, they found that only around 2% were dedicated to the collection and dissemination of child abuse imagery, suggesting as a first cut that child abuse sites are not a dominant feature (as a proportion of available content) on the Tor-hosted Darknet. However, a radically different picture emerged when they actually tracked the pattern of site visits. What they found was that the 2% of sites dedicated to child abuse imagery actually received over 80% of all the recorded site visits. Even when accounting for the activity of bots, law enforcement and returning users, it is fair to say, as Owen and Savage conclude, that 'child abuse content is the most popular type of content on the Tor Dark Net' (Owen and Savage, 2015: 9).

Additionally, the recent rash of ransomware attacks further exposes the potentially malicious use of .onion urls. When infected with ransomware, a user's device is encrypted and a pop-up screen instructs the user on how to obtain the decryption key to their device, often via a Bitcoin payment at a .onion url contained on the screen. When combined with hosted botnet command and control nodes and the various forms of online illegal content discussed above, the Darknet becomes a clear potential enabler of online crime. People who have been subject to crime in the past, therefore, should find a ready scapegoat in Dark Web technologies. This discussion suggests a fifth hypothesis:

H5. Past exposure to data breaches should increase opposition to Dark Web.

While the Darknet's ability to enable crime can affect popular sentiment, there is also empirical evidence to suggest that a user's political context matters, and that a more repressive political environment can drive people to use Tor, potentially as a means to circumvent censorship and protect privacy in the face of an abusive regime. By one estimation, repression matters so much for the use of Tor that moving from a country with a middling level of political repression, such as Venezuela, to an extremely repressive country like Uzbekistan can result in an additional 6094 Tor relay users per 100,000 Internet users per year (Jardine, 2016b). If China, with its 620 million Internet users in 2013, made this transition, the worsening political context inside the regime would lead to some 38 million new Tor Dark Web users per year, which is a substantively large

increase. Clearly, people can use Dark Web technologies in bad political circumstances to help avoid abuse.

However, rather than a more abusive political context leading to more use of Tor in a linear fashion, the actual relationship that emerges between the two tends to be U-shaped. Political repression drives usage rates the most, in other words, in both highly liberal and highly illiberal contexts. Plausibly, the effect of Internet freedom on opposition to Dark Web technologies should be an inverse mirror image of this tendency. High levels of Tor usage should presumably occur in places with comparatively low levels of opposition to the Dark Web and higher levels of opposition should correspond to political spaces with comparative lower levels of use. This logic suggests a final hypothesis:

H6. The relationship between Internet freedom and opposition to the Dark Web should be shaped like an inverted-U.

The data

In 2016, CIGI released a large cross-national survey entitled The CIGI/Ipsos Global Survey of Internet Security and Trust 2016. The original data include some 24 countries. The individual-level survey data used here draw upon a major portion of that data and encompass some 17,121 Internet users in 17 countries, with the remaining seven countries being dropped for lack of data on certain key variables.[3] The data are rich, containing basic demographic details and responses to 20 questions on topics ranging from perceptions of privacy to the cost of cybercrime and corporate data practices.

The survey also includes a simple question that captures people's level of opposition to a generic version of the Dark Web. The question itself presented respondents with a short narrative, describing the mixed picture of the Dark Web that captures the network's content, noble uses and potential abuses. More precisely, the question asked respondents the following:

> A part of the Internet known as the 'Dark Net' is only accessible via special web browsers that allow you to surf the web anonymously. Journalists, human rights activists, dissidents and whistleblowers can use these services to rally against repression, exercise their fundamental rights to free expression and shed light upon corruption. At the same time, hackers, illegal marketplaces (eg. selling weapons and narcotics), and child abuse sites can also use these services to hide from law enforcement. Do you agree or disagree that the 'Dark Net' should be shut down. (CIGI/Ipsos, 2016)

Responses to this question capture basic level of opposition to the Dark Web among Internet users. In the original survey, respondents indicated their answers along a four-point ordinal scale (strongly disagree (1) to strongly agree (4)). This data structure would necessitate the use of an ordered logistic regression. However, running a Brant Test on the results of an ordered logistic regression reveals that the parallel lines assumption of the ordered logit estimator is violated by the data. Because of the nested nature of the observations (individuals within different countries), alternative estimators such as the generalized ordered logit are not a readily viable fix for the violation of the parallel lines assumption because they do not have a mixed-effect variant. As a result, I collapsed the

dependent variable into a binary indicator, with a value of one (1) indicating a desire to shutdown the Dark Web and a value of zero (0) indicating a desire to keep it up. This allows me to use a mixed-effect logistic estimator.

Overall, the data on the dependent variable show that popular support is largely with those who wish to shutter the Dark Web. Among the 24 countries in the original sample, a majority (72%) of respondents are opposed (somewhat or strongly) to the Darknet as it was described and want it shutdown. The remaining 28% support keeping the Dark Web up and running, either somewhat (21.04%) or strongly (6.96%). Among the truncated sample of 17 countries used in this study, 73.47% of respondents wanted the Darknet shutdown, which is statistically indistinguishable from the number for the full sample.

The data for the privacy, censorship and data breach variables are taken from various substantive questions in the CIGI/Ipsos survey. *The privacy measure* is an index of respondent answers to two questions. The first question gages people's views on the legitimacy of governments accessing content data for national security purposes. The second measure assesses how people felt about governments collecting and analysing user metadata to help fight crime. Together, the content and metadata questions capture people's view towards the importance of online privacy. *The censorship measure* is operationalized via respondent answers to a question asking how much they trust that their online activities are not being censored. The exposure to *online crime variable* is measured in binary terms. The survey asked respondents to indicate if they had ever been notified that their user data had been breached. Basic weighted descriptive statistics are given below in Table 1.

The data on Internet freedom that is used to determine the potentially conditional effect of privacy and censorship concerns on opposition to the Dark Web are taken from the 2015 Freedom on the Net report (Freedom House 2015). The scores for the Net freedom index are a composite of scores on three factors: (1) barriers to Internet access within a country, (2) limitations to the access of content, and (3) the violation of privacy rights through surveillance and other methods (Freedom House 2015: 20). The aggregate scores range from 0 to 100, with 0 being the freest possible network and 100 being the least free.

The survey also contained a number of demographic questions that help to more clearly specify the effect of privacy perceptions, censorship concerns, exposure to online crime and network freedom. In particular, the survey collected data on a respondent's age, education and income levels, gender, the respondent's sector of employment and his or her marital status. Some of these factors are potentially interesting in their own rights. Including them in the regression estimations is also necessary in order to more precisely specify the effect of privacy perceptions, censorship concerns, exposure to online crime and Internet freedom on individual-level opposition to the Dark Web. Again, the weighted basic descriptive characteristics for each variable are shown in Table 1.

Quantifying the effect of privacy, censorship, online crime and network freedom on opposition to the Dark Web

What mechanisms drive people to oppose Dark Web technologies? Do individual-level privacy perceptions, censorship fears and bad experiences with online crime affect user opposition to Dark Web technologies? If so, how much do these factors matter? Moreover,

Table 1. Summary statistics (weighted).

	Obs	Weights	*Mean*	*Standard deviation*	Min	Max
Perceptual and experiential variables						
Privacy perceptions	17,121	8500	4.019	1.456789	2	8
Censorship concerns	17,121	8500	2.666	.8901117	1	4
Exposure to data breaches	17,121	8500	.260	.441995	0	1
Demographic variables						
Age	17,121	8500	2.842	1.353	1	5
Education	17,121	8500	2.069	.817	1	3
Income	17,121	8500	2.297	.850	1	4
Gender	17,121	8500	.496	.500	0	1
Employment variables						
Public sector	17,121	8500	.149	.356	0	1
Private sector	17,121	8500	.533	.498	0	1
Student	17,121	8500	.098	.297	0	1
Retired	17,121	8500	.061	.239	0	1
Not working	17,121	8500	.147	.354	0	1
Prefer not to answer	17,121	8500	.011	.102	0	1
Marital status variables						
Married/common law	17,121	8500	.635	.482	0	1
Country-level Internet freedom						
Freedom on the net	17,121	8500	33.176	18.726	16	88

do privacy perceptions and censorship concerns matter more in regimes with more restrictive online environments? Does the level of Internet freedom in a country itself matter for individual-level opposition to the Dark Web?

Table 2 presents the results of four hierarchical mixed-effect logit regressions using opposition to the Dark Web as the dependent variable. These models control for the clustered character of the data and allow for a clearer isolation of the average effect of each factor across the world. The relatively small number of level-two units (countries) is potentially problematic but likely not damning. Richter (2006), for example, suggests a necessary total number of level-2 units well about the 17 included in the regressions below. Yet others, such as Nezlek (2008) and Gelman (2006), maintain that fewer than 10 second-level units can be sufficient to justify the use of hierarchical models, even if there may be attendant estimation and interpretation problems for the second-level units. Ultimately, while sample size does matter and more is generally better, the log ratio test, which compares the fit of a mixed-effect model to the results of an ordinary non-hierarchical logit regression, gives us some indication of which estimator is a better fit for the data. As detailed in the models below, the log ratio tests for each model indicate that the mixed-effect models are a better fit to the data, although interpretation of the results of the country-level factors (net freedom) must be done with some caution.

Another potential estimation problem is the issue of multicollinearity. Given the variables at work in the models, there is the potential danger that factors such as age and

Table 2. Privacy, censorship, data breaches, net freedom and Dark Web opposition.

	Model 1	Model 2 (privacy/net freedom interaction)	Model 3 (censorship/net freedom interaction)
Privacy conscious	−.290 *** (.018)	−.354*** (.038)	−.289*** (.018)
Privacy by net freedom		.002** (.001)	
Censorship concerns	−.203 *** (.0299)	−.204*** (.030)	−.132** (.061)
Censorship by net freedom			−.002 (.002)
Exposure to online crime	.172 *** (.061)	.173*** (.061)	.169*** (.061)
Freedom on the net	.022 (.015)	−.002 (.006)	.012** (.006)
Freedom on the net^2	−.0002 (.0002)		
Male	−.237*** (.053)	−.236*** (.053)	−.235*** (.053)
Education	−.119*** (.036)	−.115*** (.036)	−.115*** (.036)
Income	.021 (.033)	.020 (.033)	.021 (.033)
Age	−.010 (.024)	−.011 (.024)	−.011 (.024)
Public sector	.186** (.079)	.184** (.078)	.185** (.078)
Private sector	Baseline	Baseline	Baseline
Student	−.164* (.096)	−.161* (.096)	−.161* (.096)
Retired	.266** (.123)	.261** (.123)	.267** (.123)
Not working	.113 (.080)	.116 (.080)	.114 (.080)
Prefer not to answer	.121 (.249)	.122 (.249)	.115 (.249)
Married/common law	.256*** (.061)	.254*** (.061)	.254*** (.061)
Country-level random effects portion (_cons)	.050 (.022)	.054 (.023)	.053 (.023)
Number of observations	17,121	17,121	17,121
Number of groups	17	17	17
LR test vs. ologit regression	chibar2(01) = 41.53 Prob ≥ chibar2 = .0000	chibar2(01) = 44.04 Prob ≥ chibar2 = .0000	chibar2(01) = 43.57 Prob ≥ chibar2 = .0000

LR: likelihood ratio.
***$p \geq .01$, **$p \geq .05$, *$p \geq .1$.

income might be highly correlated with one another. If present, excessive multicollinearity could inflate the standard errors and potentially bias the significance of the results. To check for multicollinearity problems, I generated a post-estimation correlation variance–covariance matrix, which displays the correlation of the coefficient estimates for the model. Somewhat surprisingly, only a single problem emerged. The coefficients of the public sector and the private sector employment variables were correlated above .50, speaking to a potential problem of minor collinearity. To correct for this issue, the models use the dummy variable for the private sector as the baseline measure for the other employment variables (a procedure that was necessary in any case). Once private sector employment was removed from the analysis, the models had no other apparent multicollinearity problems.

The results in Model 1 of Table 2 show that privacy perceptions, censorship concerns and prior exposure to online crime tend to strongly condition a person's level of

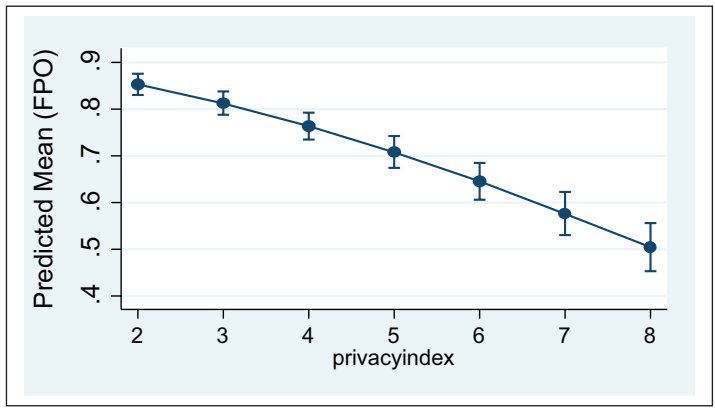

Figure 1. Privacy and Dark Web opposition.

opposition to the Dark Web. The results support *H1*, *H3* and *H5*. *H6*, specifying an expected inverted-U-shaped relationship between network freedom and opposition to the Dark Web, is not confirmed, although the direction of the signs on the coefficients for the FreeNet and FreeNet^2 terms do suggest the anticipated directionality but not the statistical significance. Given the small number of level-2 (country-level) observations, it is possible that network freedom is not significant due to an insufficient number of observations. Potentially, then, *H6* could be supported if more country-level observations were available.

H1 posits that increasing privacy perceptions should be negatively correlated with opposition to the Dark Web. This hypothesis is confirmed at the 99% level in Model 1. This result suggests the rather intuitive notion that people, at the margins, do recognize the utility and legitimacy of Dark Web technologies, such as Tor, for protecting individual privacy. Estimation of marginal effects provides a way to depict the substantive effect of changes in respondent privacy perceptions and their degree of opposition to the dark web, while holding all the other factors in the model at their means for the fixed effects portion of the model (FEO). Figure 1, for example, indicates that the mean likelihood that a person would oppose the Dark Web drops from 85.23% for those will little concern with privacy to 50.41% for those who are very concern with privacy. Privacy perceptions, in other words, are both a statistically significant predictor of less opposition to the Dark Web and a substantively important one.

H3 posits that higher levels of concern over online censorship should again be negatively correlated with opposition to the Dark Web. As indicated in Model 1, the hypothesis is supported. Since technologies such as Tor are widely hailed as an effective censorship circumvention tool, this result suggests that growing concern over censorship is a likely mechanism by which people come to support Dark Web technologies. Again, the simple statistical significance of censorship variable reveals little about the substantive effect of the variable, but the estimation of marginal effects reveals more. Figure 2, for example, plots the mean predicted values for movement along the four levels of the censorship variable. In this case, moving from the lowest level of concern over online

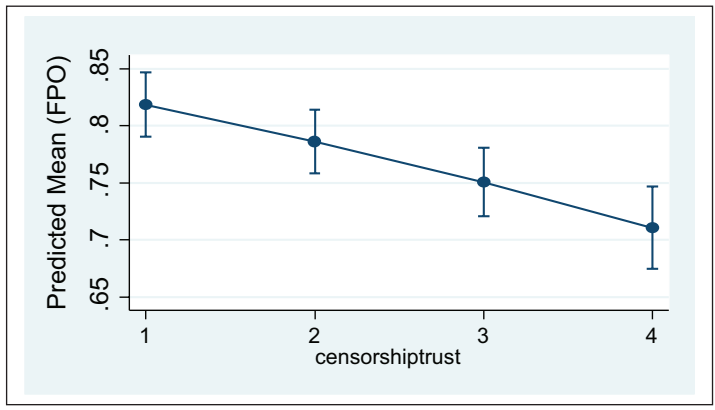

Figure 2. Censorship and Dark Web opposition.

Figure 3. Online crime and Dark Web opposition.

censorship (1) to the highest level (4) decreases people's mean opposition to the Dark Web by 10.78 percentage points, driving down the mean likelihood that someone wants to shutdown the Dark Web from 81.85% to 71.07%.

H5 posits that people with prior exposure to online crime will be more likely to oppose the Dark Web. Once again, the results in Model 1 confirm this supposition. Exposure to online crime, particularly in the case of data breaches and identity theft, strongly disposes people against Dark Web technologies such as Tor that can be used by villainous actors for malicious purposes. Figure 3 points to substantive effect exposure to crime has on public attitudes and shows how a person who has been subject to a data breach is more likely to oppose Dark Web technologies than someone whose data have not been compromised. In more precise terms, with all other factors at their mean, a person who has never had their personal data stolen has a 75.48% mean likelihood of opposing the Dark Web, while a person whose data have been breached at

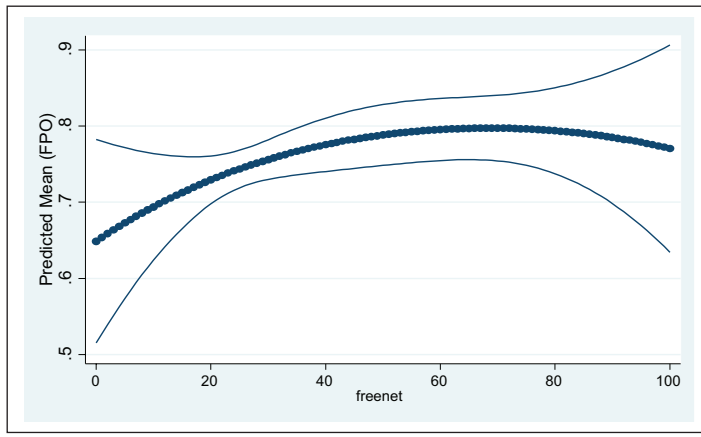

Figure 4. Network freedom and Dark Web opposition.

some point in the past has a 78.51% mean likelihood of wanting to shutdown Dark Web anonymity-granting technologies.

H6, for its part, maintains that the relationship between a country's level of Internet freedom and opposition to the Dark Web ought to be shaped like an inverted-U. This hypothesis is not statistically supported by the results in Model 1, as the interaction terms are not significant. However, the direction of the signs for the FreeNet and FreeNet^2 variables do still suggest that the relationship between state-level Internet freedom and opposition to the Dark Web may still form an inverted-U-shaped pattern.

Despite the lack of strict statistical significance for the network freedom variables, plotting their mean predicted margins is still indicative of the sort of relationship that might be at play – the relationship proposed in *H6*. Figure 4, for instance, plots the predicted margins and demonstrates the emergence of the inverted-U-shaped pattern. The mean predicted opposition to the Dark Web starts at 64.88% in the freest possible countries (Freenet = 0). In the most restrictive regimes (Freenet = 100), the mean predicted opposition to the Dark Web is 77.21%. The highest level of predicted opposition, however, is at a middling value on the Freedom on the Net 100-point scale. More precisely, when network freedom is equal to 70, the predicted mean opposition to Dark Web technologies reaches a peak of 79.74%. This pattern is broadly in line with the U-shaped relationship between Tor usage rates and political repression uncovered by Jardine (2016b). Plausibly, more observations at the state level are needed to reveal the true relationship between network freedom and opposition to Dark Web technologies.

The results have more nuanced implications for the conditional hypotheses *H2* and *H4*. *H2* posits that privacy concerns should have the largest material impact on levels of opposition to the Dark Web in more repressive regimes. The logic, here, is that in places where privacy is most challenged, it will be held in highest esteem, leading, in turn, to higher levels of support for Dark Web technologies that can help protect individual users.

As indicated in Model 2, interacting network freedom and privacy perceptions does produce a statistically significant result at the 95% level. This finding suggests that a

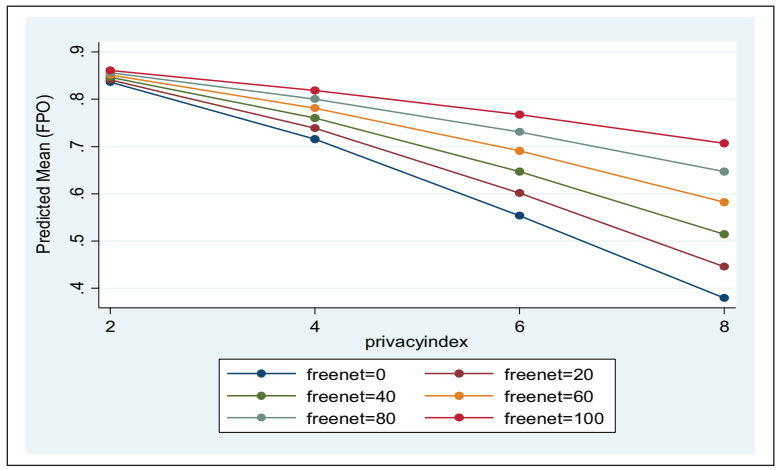

Figure 5. Privacy, network freedom and opposition to the Dark Web.

person's overarching context does indeed affect the degree to which his or her privacy concerns translate over into declared opposition to Dark Web technologies. However, as indicated in Figure 5, it turns out that *H2* had the relationship backwards. Rather than network restrictions amplifying privacy concerns, the empirical results indicate that *network freedom* tends to instead amplify privacy's effect on declared levels of opposition to Dark Web technologies. In this sense, network freedom and technologies that can be used to secure freedom on the net are mutually reinforcing. Moreover, network freedom's conditioning effect tends to be most pronounced when individuals hold very strong views of the importance of privacy.

H4 – that censorship concerns should be most amplified in more restrictive regimes – is statistically disconfirmed, but only strictly so. While increased censorship concerns tend to decease opposition to Dark Web technologies in each overarching political context, the anticipated amplification effect of network restrictions is observable. People in more restrictive political environments are overall more hostile to Dark Web technologies, but the rate at which growing censorship concern reduces that opposition is more pronounced in repressive countries than in freer, more liberal regimes. Figure 6, for example, reveals that, within highly repressive regimes, movement from very little concern with censorship to a lot of concern reduces opposition to Dark Web technologies by roughly 15 percentage points. In contrast, a similar move in a highly liberal country results in in a reduction in opposition of around 8 percentage points. In this very clear sense, the numbers do suggest that the rate at which concern over censorship matters tends to be amplified by a worse political context. Why this happens for censorship and not privacy concerns is an interesting, as yet unsolved, puzzle.

The evidence suggests, therefore, that both *H2* and *H4* are, as stated at least, incorrect. Rather than online repression amplifying pre-existing privacy perceptions or censorship concerns, network freedom tends to act as a proverbial megaphone. One potential explanation for this result is that the political (network) freedom often associated with freer

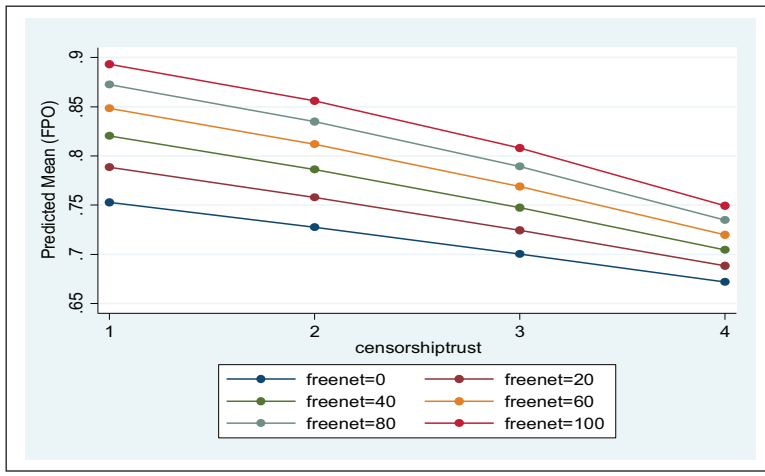

Figure 6. Censorship, repression and Dark Web opposition.

Table 3. The general profile of Dark Web supporters and opponents.

Supporters	Opponents
Privacy conscious	Less privacy concerned
Censorship concerned	Less censorship concerned
No experience with online crime	Negative exposure to online crime
Male	Female
Highly educated	Less well educated
Students	A public sector employee or retired
Single	Living married or common law

Internet environments might make people more comfortable with declaring support for a technology that can so obviously be used for nefarious purposes. There could be a virtuous cycle or proverbial Matthew Effect at play, where network freedom tends to bolster sentiment that helps to keep networks free.

The models suggest three mechanisms that lead to greater or lesser levels of opposition to Dark Web technologies. Privacy perceptions, censorship concerns and exposure to online crime all matter statistically and substantively. More broadly, the cumulative result of the models suggests a clear portrait of a Dark Web supporter or opponent. As shown in Table 3, supporters of the Dark Web are, in general, privacy conscious, concerned with censorship, free from negative experiences with online crime, male, highly educated, students, single and living in either highly free or not free regimes. Opponents tend to be less concerned with privacy and censorship, less well-educated, female, work for the public sector or retired, live common law or married, have previous exposure to online crime and live in countries with medium levels of network restriction.

Conclusions for research, public policy and the 'going dark' debate

With ongoing debates about what digital technologies should be allowed, especially in liberal democracies, the potential role of public opinion in shaping the outcome of debates on the use and development of digital technologies cannot be underplayed. While most people (73.47%) are opposed to Dark Web technologies that can be used for both noble and nefarious purposes, this top-level result masks some important underlying dynamics to do with how people actually come to oppose Dark Web technologies in the first place.

People oppose the Dark Web in some pretty consistent patterns. In general, heightened privacy perceptions tend to decrease strong opposition to the Dark Web by 34.82 percentage points. Increased concerns over online censorship likewise decrease strong opposition to the Dark Web by 10.78 percentage points. Past exposure to online crime, in contrast, increases strong opposition to Dark Web technologies by 3.03 percentage points. Network freedom, for its part, forms the expected inverted-U-shaped pattern but is not statistically significant. Moreover, the interaction of privacy concerns and network freedom does tend to result in a more pronounced effect, but rather than repression amplifying privacy perceptions, network freedom tends to bolster the effect of growing privacy concerns, suggesting a potential 'Matthew Effect'. The interaction of censorship concerns and network freedom is not statistically significant, but the general pattern suggests that network restrictions and censorship concerns are potentially synergistic.

The mechanisms driving opposition to Dark Web technologies uncovered here suggest some potential long-term forecasts for the political landscape, structuring the development and use of digital technologies. For instance, if cybercrime continues to proliferate, affecting more and more people over time, then the models developed here suggest that opposition to Dark Web technologies will continue to mount. Similarly, if today's youth really are less concerned with privacy than older generations, then, again, more people will come to oppose Dark Web technologies going forward as people's privacy perceptions become less salient. All this suggests that public opinion might be on a collision course with the current trajectory of technological development as it edges towards higher levels of encryption and, in some areas at least, more anonymity. The results also suggest that those who advocate for 'back doors' in encryption or limitations on the use of anonymity-granting technologies could become further emboldened over time as public opinion potentially swings even more in favour of shutting down Dark Web technologies.

Acknowledgements

The author would like to thank the anonymous reviewers of New Media & Society, plus Bill Graham, Gordon Smith, Fen Hampson, Leanna Ireland and Jason Kelly for their very helpful comments on various aspects of this project. If there are lingering errors, they are my own doing.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The survey data upon which this article is based were collected by the

CIGI and the global polling firm Ipsos. The survey was partially funded by Microsoft Corporation and the International Development Research Council (IDRC). CIGI retains the copyright to the data.

Notes

1. In this article, I explain the mechanisms leading to opposition to Dark Web technologies, which include everything from the Tor browser package to Darknet sites, along with other associated technologies from platforms like I2P and Freenet. When referring to the specific part of the Dark Web and Darknet, I focus on the Tor network. In particular, I use the term Darknet to refer to non-web content hosted on .onion urls and hidden services on the Tor network. I use the term the Dark Web to refer to the broader world of anonymized Internet activity, including hosting web content but also anonymized browsing of the surface web via the Tor browser.
2. While the full definition is presented in detail later, for the immediately curious reader, the definition of the Dark Net used in the CIGI/Ipsos survey is

   > A part of the Internet known as the 'Dark Net' is only accessible via special web browsers that allow you to surf the web anonymously. Journalists, human rights activists, dissidents and whistleblowers can use these services to rally against repression, exercise their fundamental rights to free expression and shed light upon corruption. At the same time, hackers, illegal marketplaces (eg. selling weapons and narcotics), and child abuse sites can also use these services to hide from law enforcement. Do you agree or disagree that the 'Dark Net' should be shut down. (CIGI/Ipsos, 2016)

3. The studied countries included Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, India, Indonesia, Italy, Japan, Mexico, South Africa, South Korea, Turkey and the United States. The full 2016 survey also includes Sweden, Poland, Hong Kong, Tunisia, Pakistan, Nigeria and Kenya, which are missing values for this study.

References

Barth B (2016) Public opinion split on whether hacktivists have legit place in society. *SC Magazine*. Available at: https://www.scmagazine.com/public-opinion-split-on-whether-hacktivists-have-legit-place-in-society/article/529083/

Biryukov A, Pustogarov I, Thill F and Weinmann R-P (2013) Content and popularity analysis of Tor hidden services. In: Proceedings of IEEE symposium on security and privacy, San Francisco, CA, 19–22 May. Available at: https://arxiv.org/pdf/..pdf13086768

Burstein P (2003) The impact of public opinion on public policy: a review and an agenda. *Political Research Quarterly* 56(1): 29–40.

CIGI/Ipsos (2016) CIGI/Ipsos Global Survey of Internet Security and Trust. Available at: https://www.cigionline.org/internet-survey-2016

Cox J (2015) The FBI's 'Unprecedented' hacking campaign targeted over a thousand computers. *Motherboard*. Available at: http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers

Freedom House (2015) Freedom on the Net 2015: privatizing censorship, eroding privacy. Available at: https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf

Gehl RW (2016) Power/freedom on the Dark Web: a digital ethnography of the Dark Web social network. *New Media & Society* 18(7): 1219–1235.

Gelman A (2006) Prior distributions for variance parameters in hierarchical models. *Bayesian Analysis* 1(3): 46–63.

Global Drug Survey (2016) Key findings from the Global Drug Survey 2016 (data collected Nov 15–Jan 16). Available at: https://www.globaldrugsurvey.com/past-findings/the-global-drug-survey-2016-findings/

Greenberg A (2014) Why Facebook just launched its own 'Dark Web' site. *Wired*. Available at: https://www.wired.com/2014/10/facebook-tor-dark-site/

Greenberg A (2016) Dark Web's got a bad rep: 7 in 10 people want it shut down, study shows. *Wired*. Available at: https://www.wired.com/2016/03/study-finds-7-10-people-want-dark-web-shut/

Hampson F and Jardine E (2016) *Look Who's Watching: Surveillance, Treachery and Trust Online*. Waterloo, ON, Canada: Centre for International Governance Innovation Press.

Higgins KJ (2013) Botnet behind mysterious spike in Tor traffic. *Dark Reading*. Available at: http://www.darkreading.com/attacks-breaches/botnet-behind-mysterious-spike-in-tor-traffic/d/d-id/1140422?itc=edit_in_body_cross

Human Rights Watch (2006) Race to the bottom: corporate complicity in Chinese Internet Censorship. *Human Rights Watch* 18(8). Available at: https://www.hrw.org/reports/2006/china0806/china0806web.pdf

Intelliagg (2016) Deeplight: shining a light on the Dark Web. Available at: http://media.scmagazine.com/documents/224/deeplight_(1)_55856.pdf

Jardine E (2015) The dark web dilemma: Tor, anonymity and online policing. Global Commission on Internet Governance paper, Series no. 21, pp. 1–13, 30 September. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711

Jardine E (2016a) A continuum of Internet-based crime: how the effectiveness of cybersecurity policies varies across cybercrime types. In: Olleros FX and Zhegu M (eds) *Research Handbook on Digital Transformations*. Northampton, MA: Edward Elgar. Available at: http://papers.ssrn.com/sol/papers.cfm?abstract_id=32704434

Jardine E (2016b) Tor, what is it good for? Political repression and online anonymity-granting technologies. *New Media & Society*. Epub ahead of print 31 March. DOI: 10.1177/1461444816639976.

Jenning B, Schwartz O and Fresco S (2015) How dark net arms dealers could easily smuggle assault weapons to Paris. *Vocatvi*. Available at: http://www.vocativ.com/250711/isis-paris-attacks-guns-dark-net/

Moore D and Rid T (2016) Cyrptopolitik and the darknet. *Survival*, 58(1): 7–38.

Muffett A (2016) 1 million people use Facebook over Tor. *Facebook*. Available at: https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648

Nezlek JB (2008) An Introduction to multilevel modeling for social and personality psychology. *Social and Personality Psychology Compass* 2(2): 842–860.

Owen G and Savage N (2015) The Tor dark net. Global Commission on Internet Governance paper, Series no. *20*, 30 September, pp. 1–9. Available at: https://www.ourinternet.org/sites/default/files/publications/no20_0.pdf

Richter T (2006) What is wrong with ANOVA and multiple regression? Analyzing sentence reading times with hierarchical linear models. *Discourse Processes* 41: 221–250.

Sharpe A (2016) Global majority backs a ban on 'dark net', poll says. *Reuters*. Available at: http://www.reuters.com/article/us-tech-privacy-idUSKCN0WV111

Tor Project (2015) Some statistics about onions. *Tor Blog*. Available at: https://blog.torproject.org/blog/some-statistics-about-onions

Tor Project (n.d.) Who uses Tor?. Available at: https://www.torproject.org/about/torusers.html.en

Tracy A (2016) 71% of people globally think the dark net should be shut down. *Forbes*. Available at: https://www.forbes.com/sites/abigailtracy/2016/03/30/majority-of-people-globally-dark-net-shut-down-silk-road-tor/#31f9265a2461

Viebeck E (2016) U.S. hacks San Bernardino iPhone; majority supports ban on 'dark net'; why ISIS is winning the online messaging war. *The Washington Post*. Available at: https://www.washingtonpost.com/news/powerpost/wp/2016/03/29/u-s-hacks-san-bernardino-iphone-majority-supports-ban-on-dark-net-why-isis-is-winning-the-online-messaging-war/?utm_term=.82259fb8407d

Author biography

Eric Jardine is an assistant professor of Political Science at Virginia Tech and a CIGI Fellow. His research focuses on human-computer interaction as it pertains to information security and data protection, as well as the use and abuse of anonymity-granting technologies.