Subverting Surveillance or Accessing the Dark Web?
Interest in the Tor Anonymity Network in U.S. States, 2006-2015

Andrew M. Lindner
Skidmore College, Saratoga Springs, NY

Tongtian Xiao
Columbia University, New York, NY

Abstract

The U.S. government engaged in unprecedented forms of mass surveillance in the 21st century. Users of the The Onion Router (Tor), an anonymity-granting technology, mask themselves from state surveillance and can gain access to illicit content on the Dark Web. Drawing on theory regarding “exposure” to surveillance, this study examines how two issue-attention cycles (related to the Edward Snowden state surveillance revelations and the Dark Web respectively) are associated with public interest in the Tor browser in the U.S. Using data at the state-year level from 2006-2015, this study estimates fixed effects models, controlling for socio-demographics, the presence of journalism, tech, and political jobs, as well as multiple measures of state political ideology. The results indicate that state-years with greater popularity of Google searches related to the Snowden story had significantly higher popularity of searches for Tor. By contrast, there was no association between Dark Web search popularity and Tor search popularity. These findings are consistent with the notion that the Snowden incident increased Americans’ sense of exposure, leading to interest in anonymity-granting technology.

Corresponding author:

Andrew M. Lindner, Department of Sociology, Skidmore College, 815 N. Broadway, Saratoga Springs, NY 12866. Email: alindner@skidmore.edu.

Acknowledgements:

The authors thank Stephen Barnard, John Brueggemann, and Eric Jardine for their helpful comments.

INTRODUCTION

On March 15, 2013, according to his own account of the events, Edward Snowden smuggled a flash drive out of the NSA regional facility in Kunia Camp, Hawaii where he had worked for the past year. Snowden, a contractor for the government consulting firm, Booz, Allen, Hamilton, Inc., had grown increasingly concerned about the bulk collection of private citizens' emails, phone records, search histories, text messages, and photos (Jauch 2014). That flash drive's contents, which Snowden would soon turn over to journalists in a Tokyo hotel room, included a cache of documents offering alleged evidence of U.S. intelligence agencies' conducting surveillance on millions of Americans.

Of course, state surveillance is nothing new. States have long exercised social control over their citizens whether through networks of informants, search and seizure, and CCTV. While some intelligence officials, journalists, and academics contest aspects of Snowden's claims (Gros, de Goede, and İşleyen 2017), what his release of classified documents certainly accomplished was to bring greater public attention to the under-reported issue of state surveillance, potentially making people more aware of their own vulnerability. In the years following the Snowden disclosures, references to mass surveillance have been common in popular culture with references in TV shows like *Black Mirror* and *House of Cards* and even a feature film about Snowden directed by Oliver Stone.

Given the recent attention to various forms of surveillance, it is unsurprising that most Americans think that the U.S. government is monitoring their phones and emails. Yet, many report that they lack the necessary knowledge to use digital technologies to protect their privacy (Olmstead 2017). A number of user-friendly technologies, including VPN servers and anonymous search engines, now make it easy for citizens to have some degree of online privacy. But, to have greater protection from the spying eyes of states and hackers, somewhat more complex technologies, like The Onion Router (Tor), are necessary. For these reasons, Tor has garnered *caché* with civil liberties and privacy advocates as well as newspapers like *The New York Times* and *The Guardian*, which invite would-be whistleblowers to use Tor to leak files on their Deep Web sites (Marx 2016; Jardine 2016).

At the same time, Tor is also the dominant gateway to access a range of illicit activities on the Dark Web¹. A growing body of research has documented the proliferation of cryptomarkets where drugs, arms, and hacked account information are available (Jardine 2015; Barratt 2012). Other research has shown the largest share of Dark Web traffic is directed to child abuse imagery sites (Owenson and Savage 2015). The Dark Web, too, has had its fair share of popular culture appearances, including the sadistic horror movie, *Dark Web*, and its equally mindless and gory sequel.

These are the two dominant stories about Tor. In one story, Tor is a tool for maintaining one's privacy in the face of the state's growing surveillance apparatus. In the other, Tor is a gateway to the Web's seedy, digital underbelly where all manner of illicit activities are possible. Both stories are true in some measure. Offering a privacy shield and creating an access point for the Dark Web are both "digital affordances" of Tor (Davis and Chouinard 2016). And, to be sure, they are not mutually exclusive; online and in physical spaces, people engaged in illicit activities

often seek to dodge surveillance. But the two stories offer different motivations for using Tor and may appeal to different potential constituencies of Tor users.

In this study, we examine whether interest in state surveillance (as measured by the popularity of Google searches related to Edward Snowden) or interest in the Dark Web best accounts for public interest in Tor. Nominally, this is a study about the issue-attention cycles that raise people’s awareness of a software program. But the implications are potentially profound. The findings offer us initial, ecological evidence that offers clues about the bigger question of when and why citizens take measures to shield themselves from state power in the form of surveillance. Do state-years with greater interest in the Snowden revelations, a story that highlighted state surveillance, have greater interest in Tor? Or is interest in Tor more closely associated with the emergent Dark Web?

We begin by reviewing existing literature on the sociology of surveillance and the adoption of anonymity-granting technologies. Next, we introduce a new state-year dataset, which pulls together data from Google Trends, the American Community Survey (ACS), the Bureau of Labor Statistics (BLS), and Correlates of State Policy Project at Institute for Public Policy and Social Research (IPPSR). Then, we describe the results of a state and time fixed effects model, controlling for socio-demographics, the presence of journalism, tech, and political jobs, as well as multiple measures of state political ideology. The results of this research contribute to an incipient body of literature on Americans’ technological responses to growing concerns regarding cybersecurity and state surveillance.

LITERATURE REVIEW

Sociology of Surveillance

The social control of individuals through surveillance has a history that begins long before the era of powerful computers, Internet connectivity, and social media sharing. But since the 1970s, surveillance “has emerged as the dominant organizing practice of late modernity” (Lyon, Haggerty, and Ball 2012:1). The broad term, “surveillance,” includes a wide variety of practices that range from the use of CCTVs and police body cams to companies tracking their employees’ web browser histories to individuals surveilling their own friends’ activities on social media. Even as these various forms of surveillance have expanded, the mass collection of data by the state has grown at an especially staggering rate.

Of particular interest for our purposes is the notion of “dataveillance,” a term first coined by Clarke (1988:2), which refers to “the systematic use of personal data” to monitor the activities and communications of individuals. As Marx (2016) notes, “the world is awash in new kinds of data” (pg. 49) When these forms of data, whether it be bank transactions, medical information, or personal communications, are made digital, they can be communicated widely and statistically analyzed on a previously unimaginable scale (Marx 2016). Haggerty and Ericson (2003) describe the contemporary paradigm using the concept of “surveillant assemblages,” a collection of machines and operations, which analyze and sort objects (e.g., images, recordings, messages, digital networks) disembodied from physical people in a geographical space. As they write, “Today, surveillance is more in keeping with the technological future hinted at by Orwell, but

augmented by technologies he could not have even had nightmares about” (pg. 612). These machinic and algorithmic approaches to surveillance have, at times, allowed analysts at intelligence agencies to leap from examining a suspect’s photos to reading his cousin’s sister’s emails. Contemporary surveillance, including dataveillance, can expand indefinitely through social networks to draw more people into its gaze.

Several consequences flow from the capacity of states and corporations to conduct dataveillance. First, as van Dijck (2014) observes, “whereas surveillance presumes monitoring for specific purposes, dataveillance entails the continuous tracking of (meta)data for unstated preset purposes” (pg. 205). Second, the scale of “big data” allows for the vast accumulation of personal data, which, in turn, allows for an industry of “big data analytics” and data mining (Degli Esposti 2014). These analytics allow firms to engage in subtle forms of behavioral modification, creating a “feedback loop” of data collection, digital “nudges,” and further dataveillance (Degli Esposti 2014). Finally, as is suggested by the term, *mass* surveillance, there has been a trend toward “the democratization of surveillance.” It is important to note that both historically and currently states have targeted members of racial, ethnic, religious, ideological, and other minorities groups for surveillance to a greater extent. Moreover, members of more affluent and privileged groups are more likely to have the digital literacy and access to technologies necessary for resist surveillance (Marx 2016). For these reasons, surveillance both produces and reinforces inequalities. Still, it is almost impossible to imagine someone who fully participates in modern life being able to avoid surveillance altogether.

Within this context, much has changed about the power dynamics and social contract between the individual, corporations, and the state (van Dijck 2014). The diffusion and integration of technologies into nearly every facet of social life and the enormous amount of data collected by private companies (e.g., Google and Facebook, Internet service providers (ISPs), cell phone companies, employers, etc.) has meant a blurring of boundaries between private entities and the state. Today’s surveillance apparatus is a radically de-centralized system composed of private companies collecting data, municipal and private CCTV systems, and private citizens recording pictures and videos of each other. Authorities gain access to these data, but are not necessarily the primary collectors of it. Such companies now “provide authorities with routine access to data about their clientele” (Lyon et al. 2012:3).

Many police, security firms, intelligence agencies, and regulators argue that dataveillance combined with a steady flow of information from private companies to the state allows for stronger national security, crime detection, and financial security (Clarke 1988). Of course, this rationale for state mass surveillance took on new salience in the post-9/11 era. The “War on Terror” offered political and practical justifications for an expansive surveillance infrastructure to promote national security, normalizing an array of new surveillance practices especially the US and UK governments (Amoore and De Goede 2005; Marx 2016; van Dijck 2014). However, many scholars and commentators see these increased surveillance and dataveillance practices as a clear shift in power toward the state and away from individual privacy rights (Clarke 1988; Murakami Wood and Webster 2009; van Dijck 2014).

Managing Exposure

How do people respond to surveillance? A longstanding view of police departments is that surveillance promotes criminal deterrence (Marx 2003). People are less likely to speed on the highway if they know the police are watching. But, by the same logic, various forms of surveillance may deter behavior that is not criminal, merely stigmatized. The central concern of many civil liberties advocates is that a growing surveillance state may deter perfectly legal forms of behavior, thought, and expression due to fear of exposure (Ball 2009; Marx 2016). For precisely this reason, new forms of surveillance often yield not only deterrence, but also new waves of resistance against them.

In other words, responses to surveillance are not binary or predictable. As Ball (2009) argues, people respond to surveillance with a more complex and varied set of reactions. Some people are enthusiastic about surveillance for ideological or patriotic reasons. Other people may put up with it because they believe it is necessary for their safety. And some people actively resist surveillance. Ball (2009) introduces the theoretical concept of “exposure” to describe the subjective experience of being surveilled and considers various factors that may contribute to a greater sense of feeling vulnerable and exposed. Feeling a sense of “exposure” depends, among other factors, on awareness of surveillance in the first place, the invasiveness of the data being collected, and how much the person has absorbed rhetoric which legitimates surveillance (e.g., “if you have nothing to hide, you have nothing to fear”).

In the post-9/11 era, even as mass surveillance ramped up dramatically, a perfect storm of conditions took hold, minimizing the public’s sense of exposure. While some forms of surveillance are quite visible, much of the public views surveillance as a mundane feature of contemporary life. Citizens are increasingly aware that surveillance cameras are everywhere. As Murakami Wood and Webster (2009) argue, “the lack of opposition to, or even enthusiasm for CCTV” in the UK was due, in part, to the sense that “‘something is being done’” (pg. 263). CCTV, a highly visible form of surveillance, was justified as a response to the threats of terrorism and crime. At the same time, the uneventful experience of seeing CCTVs mounted on every corner also served to normalize surveillance. Bush and Blair administration officials often couched their rhetoric regarding mass surveillance in appeals to terrorism risk mitigation and patriotism, which served to legitimate the practices (Lyon 2003; Amoore and De Goede 2005). Where people did notice surveillance, they may have seen it as a legitimate policy response or have accepted it as normal.

Ironically, the surveillance practices of the current period have “become simultaneously more visible and invisible” (Lyon et al. 2012:2). Though some forms of surveillance were highly visible, much of dataveillance of the post-9/11 era as conducted by police and intelligence agencies is essentially invisible to members of the public. Until the “wakeup call” of the Snowden disclosures, few knew just how extensive or invasive intelligence agencies’ searches were (van Dijck 2014; Lyon 2003). It is impossible to feel a sense of exposure if you are unaware of surveillance.

The growth of the “War on Terror” and mass surveillance practices occurred alongside the expansion of social media sites and broader dataveillance practices. van Dijck (2014) claims that the growth of dataveillance is closely tied to the “normalization of datafication” in which citizen-consumers allow their social behaviors and private information to be transformed into social data

and shared with other individuals and corporations. Or, as Lyon et al. (2012), put it: members of the public got into the habit of “cheerfully and voluntarily expos[ing] their data to others” (pg. 4). If it becomes common practice to share photos with online friends and strangers by posting on Instagram, individuals may perceive less exposure when the state has access to those photos. Drawing on Ball’s (2009) conceptualization, all of these factors may have contributed to reducing the public’s feeling of “exposure” to surveillance.

To the extent that people experience “exposure,” they tend to adopt strategies to manage surveillance. Marx (2003) introduces a typology of eleven “moves” that people employ to resist surveillance. These strategies include “discovery moves,” through which people attempt to verify that they are, in fact, being surveilled, and “avoidance moves,” where people avoid behaviors or settings that allow them to be surveilled. Using Tor, is what Marx refers to as a “masking move,” or subverting surveillance by shielding one’s identity. A criminal on the lamb might engage in a “masking move” by putting on a wig and fake mustache. On the Internet, Tor allows users the most secure of masks for their digital identity by participating in a “distributed masking move” which involves employing multiple servers (Dupont 2008:273). In the next section, we describe anonymity-granting technologies and consider the reasons people use them.

Anonymity-Granting Technologies

Though technologies have been crucial as states expand their mass surveillance apparatus, the same technologies, including the relative openness of an Internet independent of state control, have also generated opportunities for citizens to resist surveillance (Marx 2016). Growing mass surveillance coexists with technological responses to it. Tor has become one of the most widely used anonymity-granting technologies since shortly after it was first introduced in 2004 (Chawki 2010). As of October 2017, Tor averages more than 2.5 million users per day, according to their official website. Tor allows people to connect to web servers through virtual tunnels run by its volunteers. Using this protocol, Tor itself claims to have no access to the unique Internet Protocol (IP) addresses nor ISPs of its users. Tor volunteers set up thousands of “relays” through which Tor users can send requests for the website they intend to visit. Then, this request will be sent to at least other two computers to make sure that the information has been relayed through at least three routes before accessing the website. Since these “relays” heavily encrypt requests, only the relays’ IPs are shown to any observers. Like all anonymity-granting technologies, Tor has vulnerabilities have been exploited by hackers and law enforcement alike to expose users in the past. Still, it remains one of the more secure means of masking one’s identity online.

By design, little is known about who uses Tor. The U.S. State Department is a partial funder of Tor due to its benefits to whistleblowers and dissidents of repressive regimes internationally (Lawrence 2014). Jardine (2016) has shown that Tor use is highest in countries with low political repression (like the United States) where people are free to use the software and in countries with very high political repression (e.g., Uzbekistan) where there is a pressing political need to mask one’s digital identity. In the U.S., where there is low political repression, Tor’s own website claims that people in industries like journalism, politics, and tech use Tor in their work. But the site also goes to great lengths to argue that “Normal people use Tor,” showing a photo of

smiling mother with her pre-teen son, resting his head on her shoulder (“Who Uses Tor?” 2017). The narrative that Tor actively promotes is one of adopting a masking move to avoid exposure. They highlight legitimate and legal uses of Tor to protect against surveilling states, corporations, and hackers.

Issue-attention Cycles: Edward Snowden

According to Tor’s own rationale, a necessary pre-condition to interest in Tor is a sense of exposure. But like many serious issues, media coverage of mass surveillance ebbs and flows. As Downs (1972) famously observed, instead of focusing on one domestic issue in a sustained way, American society has a systematic “issue-attention cycle” that strongly “influence[s] public attitudes and behaviors concerning the most key domestic problems” (pg. 38). Downs argues that social problems that have gone through the cycle will receive more public attention than in their pre-discovery stage (i.e. the time when some highly undesirable social conditions exist yet without capturing public notice or national prominence). One important issue-attention cycle that may have affected public interest in Tor was the public’s attention to Edward Snowden and his 2013 revelations of NSA mass surveillance.

Specifically, what Snowden’s revelations brought to public attention was the astonishing scope of state mass surveillance. On June 6th, 2013, when *The Guardian* (UK) began to publish a series based on documents leaked by Snowden. The documents revealed that telecommunication giant Verizon had handed over metadata collected from millions of Americans’ phone calls to the FBI and the NSA (Greenwald 2013). Further revelations exposed that the NSA had direct access to user content stored by Internet companies like Google, Facebook, Apple, etc., which cover the vast majority of Internet users’ email, search history, videos and communications networks (Greenwald and MacAskill 2013). While Snowden himself became a controversial figure, the revelations about state mass surveillance raised new concerns about the government’s unrestrained power overriding its citizens, the rule of law, and potential violations of the Fourth Amendment right to privacy (Landau 2013).

The burst of attention surrounding the Snowden leak in 2013 created a context for Americans to feel a greater sense of exposure. In response, there is evidence that some Americans adopted an avoidance move. Marthews and Tucker (2017) found that Google searches on personally and politically sensitive topics declined after the Snowden revelation in 2013. Employing a secondary analysis of Google Trends data, they observe a chilling effect on web searches for search terms that people might believe would get them in trouble with government officials. Other Americans may have responded to this sense of exposure by adopting masking moves. In a 2015 Pew survey of American adults, almost 34 percent of respondents who were conscious of surveillance had tried to hide or shield their personal information from government (Rainie and Madden 2015).

Given past research on surveillance and exposure, it stands to reason that the Snowden issue-attention cycle may have created a sense of exposure in at least some portion of Americans, leading them to adopt masking moves like using Tor. If interest in Snowden serves as a proxy for a sense of exposure, we would expect to observe more interest in Tor where there is greater

exposure among the public. Accordingly, we hypothesize (H_1) that state-years with greater public interest in Edward Snowden (as measured by Google searches) will also have higher interest in Tor, holding all else constant.

Issue-attention Cycles: The Dark Web

What Tor’s web site does not mention is that the software also has its illicit and illegal uses. Tor faces what Jardine (2015) refers to as a “Dark Web Dilemma,” or the proliferation of cryptomarkets, trolls, and online child abuse rings whose illegal activities are made possible by anonymity-granting technology. One analysis of hidden-services websites within the Tor network revealed that more than half of active websites, 1547 out of 2723, found on the Deep Web contain illicit content like illegal drug sales, human trafficking, money laundering and unlawful child pornography (Moore and Rid 2016). Research has shown a large volume of Dark Web traffic is directed to child abuse imagery sites (Owenson and Savage 2015; Chertoff 2017). Tor has also been used by extremists and Islamic militants to post recruitment propaganda and how-to information for mounting terrorist attacks (Bertrand 2015).

It is worth noting that Dark Web users have motivations apart from the sheer appeal of illicit activities. Gehl’s (2016) ethnographic study of the Dark Web Social Network (SWSN) revealed individuals using the Dark Web who were looking for many of the same forms of human connection as Facebook users, but without the loss privacy. In fact, at least some users sought a form of “disembodied communications dissociated from...markers such as race or gender” (pg. 1225). On the DWSN, Gehl also found an explicit prohibition of child pornography. Other studies of Dark Web and cryptomarket users have found a libertarian-inflected enthusiasm for the personal freedoms of the Dark Web, pleasure from having technical skills to remain anonymous (Bancroft and Reid 2017; Maddox, Barratt, Allen, and Lenton 2016). Such motivations offer alternatives or may exist alongside the allure of illicit and taboo activities. However, it is certainly the case that such forms of techno-political expression garner less media attention than the other uses of the Dark Web.

Most media attention regarding the Dark Web has focused on cryptomarkets, which offer an “eBay for drugs,” weapons, malware code, and hacked account information (Barratt 2012). Research has shown that individual cryptomarkets – including Silk Road (579 vendors in 2013), Agora (867 vendors in 2015), Evolution (2,700 vendors in 2015), and AlphaBay (1,582 vendors in 2016) – come and go as the result of raids or operators absconding with users’ cryptocurrency (Rhumorbarbe, Staehli, Broséus, Rossy, and Esseiva 2016; Paquet-Clouston, Décary-Héту, and Morselli 2018). But an analysis of thirty-five Dark Web cryptomarkets revealed that the inventory consists primarily of drugs and that the volume of both vendors and sales are growing (Soska and Christin 2015).

Until 2013, among the most notorious destinations on the Dark Web was Silk Road, a cryptomarket started in February 2011. According to one estimate, sales on Silk Road grew from \$14.4 million in mid-2012 to \$89.7 million by September 2013 (Aldridge and Décary-Héту 2014). While Silk Road briefly flourished, generating a number of news stories, the website achieved its greatest notoriety in its demise. In October 2013, the FBI raided the home of site founder Ross

William Ulbricht (a.k.a. “Dread Pirate Roberts”), arresting him, shutting down Silk Road, and seizing \$3.6 million in Bitcoin, the cryptocurrency (Roy 2013). Ironically, public attention brought to illegal marketplaces on the Dark Web by the Silk Road raid may have contributed to greater interest in such services among those who were not previously aware they existed.

Greater media attention to the Dark Web and its array of illicit services constitutes another motivation for using Tor – one that is less publicized by the Tor organization itself. Throughout the period from 2006-2015, when issue-attention cycles stirred public interest in the Dark Web and its cryptomarkets, it seems likely that it also created greater interest in Tor, the primary tool needed to access the Dark Web. For this reason, we hypothesize (H₂) that state-years with greater interest in the Dark Web, Deep Web, or Silk Road (as measured by Google search popularity) will have also have greater interest in Tor, holding all else constant.

By exploring the extent to which interest in Snowden and interest in the Dark Web are associated with interest in Tor, we can begin to understand which of the two prevailing stories is the stronger predictor of interest in the anonymity-granting browser. Of course, interest in Tor is potentially affected by a number of other factors, including the demographics, political context, and local industry representation in a state. In the next section, we discuss of number of factors that are controls in the current study. While we do not offer formal hypotheses regarding these relationships, we consider various possible patterns of interest in Tor.

State Demographics

One factor potentially shaping interest in or adoption of any technology is the demographic composition of a state. While media scholars of the 1990s often wrote of a “digital divide,” researchers have since noted a broader range of “digital inequalities,” which include not simply access to a technology, but also consistency of access and the knowledge and skills necessary to use the technology fully (Hargittai and Jennrich 2016). For relatively young, college-educated, affluent, and/or white Americans, access to the Internet has been pervasive for more than a decade and the use of complex digital tools is often an essential part of their everyday work life. By contrast, lower income Americans have inconsistent access to the Internet, losing service when their cable is turned off for non-payment (Robinson 2014). Moreover, lower income people increasingly rely on smartphones or tablets rather than full-fledged computers, which are more expensive (Katz et al. 2016). It requires low technical proficiency to search Google for “Tor.” However, considering that 39% of respondents in one U.S. poll reported never having heard of Tor, to be curious about specific anonymity-granting technologies is probably more likely with either a technically-savvy personal grapevine or a media diet that includes relatively sophisticated news outlets (Rainie and Madden 2015). For these reasons, we control for the population, population density, level of economic inequality, median household income, educational attainment, age composition, racial composition, and the rate of home broadband access in state-years.

Industries Using Tor

The official website of Tor singles out several industries that Tor in their work, namely journalists, the tech sector, and the political sector. Some journalists use Tor to facilitate the collection of information from leakers. According to one analysis of Deep Web sites, 37% are self-identified legitimate sites, such as personal blogs and journalist drop sites (Moore and Rid 2016). Both *The Guardian* and *The New York Times*, for example, operate Tor Secure Drop pages, which allow whistleblowers to share files with a measure of anonymity. Likewise, Tor can prove useful to activists and political professionals alike who aim to have surveillance in their work. In 2017, White House Press Secretary Sean Spicer launched a series of “phone raids,” forcing his staff to remove Tor, Signal, Confide, and other privacy apps from their smartphones. Prior to the raids, such anonymity-granting technologies were reportedly in widespread use among White House staffers (Karni and Isenstadt 2017). After the U.S. Supreme Court stripped most government employees of their whistleblower protections in 2006 (Stout 2006), using anonymity-granting technologies allows these government whistleblowers to expose forms of corruption without revealing their identities. Finally, for IT professionals, Tor allows them enter competitors' online resources anonymously, bypass special IP blocks, and test their own corporate firewalls and other network resources (Loshin 2013: 22). Given these potential industrial uses of Tor, we control for the proportion of jobs in journalism, tech, and politics in state-years.

State Political Context

Public interest in Tor may also be affected by the political leanings of a state. In most polls of attitudes about mass surveillance, Democrats and Republicans tend to hold similar views, with a majority opposing the mass collection of private data (Ackerman and Siddiqui 2015). The Republican Party and the conservative movement have long been internally divided over state mass surveillance. Republicans, especially during the administration of President George W. Bush, have been the most vocal advocates for enhanced state surveillance, arguing that it is an essential set of tools in the War on Terror (Hills 2006). At the same time, a substantial portion of the Republican base, notable conservative intellectuals, and even the House Freedom Caucus have expressed concerns about unchecked mass surveillance (French and Tummarello 2015). While some far right activists may perceive a need for anonymity-granting technology, moderates and many Republican elected officials are openly critical of technologies that hinder government surveillance.

The political left, by contrast, has traditionally defended individual civil liberties through both non-profit organizations like the American Civil Liberties Union (ACLU) and grassroots activism. Left-wing activists and organizations have organized most of the political opposition to state mass surveillance, most visibly taking the form of marches in New York and Washington D.C. on the twelfth anniversary of the signing of the Patriot Act in 2013. Despite these forms of activism and consistent polling showing that most Democratic voters oppose state surveillance, many Democratic elected officials voted for the Patriot Act and the Obama administration continued or expanded the surveillance practices of the Bush era NSA and HSA (Landau 2013; Bauman et al. 2014). While elements of both the left and the right may perceive a need for anonymity-granting technologies, awareness of exposure to mass surveillance may be more

widespread in more liberal contexts. For this reason, we control for the political ideology of each states' representatives and its citizens.

METHODS

In this study, we adopt an ecological approach to examining public interest in Tor. In doing so, we are able to study how concern for mass surveillance and interest in the Dark Web may contribute to interest in Tor. The data used in this study come from several sources: Google Trends, the American Community Survey (ACS), the Bureau of Labor Statistics (BLS), and political data maintained by the Correlates of State Policy Project at Institute for Public Policy and Social Research (IPPSR). The unit of analysis is state-year. Except for the political measures which have missing data for the District of Columbia (D.C.), full information was available for all fifty states and D.C. from 2006-2015. Complete descriptive statistics for all measures can be found in Table 1.

Dependent Variable

The dependent variable is a state-year measure of the Google search popularity for the topic "Tor." Data are available through Google Trends, a web utility allowing users to examine search popularity patterns over time and by geographical areas. Google Trends provides normalized, relative interest data on a per-query data. For each new query, the time or place with the peak popularity for that search term is given a value of 100. All other values are reported as percentages of that interest. For example, a state with a value of 15 has fifteen percent of the search popularity for Tor as the peak. Because the time data was reported in months and aggregated into years by the researchers, no state-year has a value of 100 (i.e., peak search popularity for Tor) for the whole year. In our data, Oregon in 2015 had the highest relative search popularity for Tor (77.08) and Louisiana in 2006 had the lowest (13.32). In Google Trends' lingo, a "topic" is a recognized "group of terms that share the same concept" (Google 2017). "Tor," "browser tor," "tor browser," and "download tor" are all terms referring to the topic of "Tor, anonymity network." The full collection of terms included in a topic is unknown. However, in series of analyses available from the authors upon request, the topic "Tor" produces more stable state-year estimates than most single Tor-related terms or even collections of several Tor-related terms.

This study makes no assumption about the proportion of people who search for Tor who ultimately download it or who end up using it regularly. Many Google searchers may simply seek a better explanation of what Tor is. Past research has shown that Internet search popularity data offer reliable and valid measures of public interest in various topics including racial animus and black candidates (Stephens-Davidowitz 2014), conspiratorial ideation (DiGrazia 2017), Tea Party mobilization (DiGrazia 2015), and the Black Lives Matter movement (Gross and Mann 2017). Following these researchers, we understand higher search popularity for Tor to mean greater public interest in Tor in a given state-year.

Independent Variables

The two measures of issue-attention cycles are also drawn from Google Trends. The first is a measure of state-year search popularity related to Edward Snowden, the NSA contractor who disclosed state surveillance methods in 2013. We used data from the oddly-titled Google Trends topic “Edward Snowden, American computer professional.” An alternative approach would have to use terms related to “surveillance,” “NSA spying program,” etc. Unfortunately, most terms related to “surveillance” are searches associated with the purchase of home surveillance equipment. Terms related to the NSA or mass surveillance were simply too rare to produce consistent state-year estimates. By contrast, there were far more searches related to Edward Snowden. In some ways, Snowden may have become a symbol for the larger issue of state mass surveillance and, therefore, it serves as a useful proxy measure in this study. Due to substantial missing data before Snowden became (in)famous at the time of his disclosures, we followed a procedure first introduced by DiGrazia (2015).ⁱⁱ The other issue-attention variable was search popularity related to the Dark Web. Using Google Correlate, a tool for finding corresponding search terms, we identified “Deep Web” and “Silk Road” as closely related to “Dark Web.” Consequently, we produced a measure that takes the average of state-year search popularity for each of the three.

The demographic measures are population (in 10,000s), population density (logged), Gini coefficient, percent white, percent with a college degree or higher, percent under age 35, and percent with home web access. Except for the web access variable, all measures were drawn from the American Community Survey 1-year estimates (2006-2015). The web access variable was drawn from the Current Population Survey (CPS). Due to missing data, values for years 2006 and 2008 were interpolated based on years 2005, 2007, and 2009. All percentages and the Gini coefficient are represented on a 0-100 scale.

The two measures of state political context were drawn from Correlates of State Policy Project at Institute for Public Policy and Social Research (IPPSR). Citizen state ideology, a 0 to 100 measure developed and maintain by Berry and Ringquist (1998), is “generally conceived as the mean position on a liberal-conservative continuum of the “active electorate” in a state” (pg. 327). More liberal states are coded higher with Vermont in 2006 having the most liberal citizen ideology. The other variable is a NOMINATE measure of state government ideology, which makes use of the widely used NOMINATE system maintained by Keith Poole (<https://voteview.com/>). As with the other measure, more liberal state governments are coded high with Massachusetts in 2009 having the most progressive state government (0-100). Data were not available for Washington D.C. on either of these measures. For that reason, for all analyses including the political measures, $n=500$ (50 states * 10 years) rather than 510 (50 states and D.C. * 10 years).

Finally, this study makes use of three measures drawn from the Bureau of Labor Statistics: the percentages of journalism jobs, tech jobs, and legislative employees in the state-year. Each of these variables is measured on a 0-100 scale.

Analytic Approach

Due to the hierarchical nature of these data, we estimated a state and time fixed effects model to examine the association between Tor search popularity and issue-attention cycles,

demographics, political context, and industries.ⁱⁱⁱ The state fixed effects remove unobserved time-constant influences, while the inclusion of year fixed effects removed unobserved time shocks common to all states. As a robustness check, the model was progressed one-at-time in various sequences and assessed for model fit.^{iv} Two models were estimated: the first includes the Washington D.C. cases, but excludes the political measures and the second includes the political measures while dropping the D.C. cases.

RESULTS

Between 2006 and 2015, public interest in Tor as measured by relative Google search popularity grew substantially reaching a peak in 2014. Figure 1 depicts the unweighted average of state search popularity for “Tor” by year. This national growth disguises substantial variation between and within states. Figure 2 illustrates this point with a series of kernel density plots for each state, arranged by mean annual Tor search popularity. Georgia, for example, the state with the lowest average public interest in Tor, had a normally distributed set of Tor search popularity scores for the observed period. By contrast, Wyoming and Vermont, which had the fourth and fifth highest mean search popularity for Tor, have bi-modal distributions, with some years falling far below the state mean and others fall well above it. Still, as Figure 3 reveals, the broad story for most states is growing search popularity for Tor until 2014, followed by a slight decline in 2015.

In the state and time fixed effects regression model (Table 2), we are able to address the non-independence of states. Recall that the first model excludes the political measures, but includes Washington D.C. in the sample ($n=510$), while the second model includes the political measures, forcing us to drop the ten D.C. cases (which have missing data on those measures). H_1 held that state-years with greater public interest in Edward Snowden (as measured by Google searches) will also have higher interest in Tor, holding all else constant. The findings support this hypothesis as search popularity related to Edward Snowden was statistically significant in both models ($p<.05$). In model 2, when controlling for political composition, for each 10% increase in searches related to Snowden, there was a 7.4% increase in searches related to Tor. The magnitude of the effect is modest, but this result offers some initial evidence that the Snowden issue-attention cycle may have contributed increased public interest in Tor.

Our second hypothesis (H_2) asserted that state-years with greater interest in the Dark Web, Deep Web, or Silk Road (as measured by Google search popularity) will have also have greater interest in Tor, holding all else constant. Across both models, Dark Web search popularity was not significantly associated with Tor search popularity. For this reason, we must reject the hypothesis.

Turning to our controls, there were substantial year effects. In model 1, holding all else constant, states in 2014 had 24.5% higher search popularity for Tor compared with 2006, the reference year ($p<.001$). Interest in Tor, as measured by Google search popularity, has quite clearly grown since 2006. Few of the demographic conditions in states were associated with Tor search popularity. Holding all else constant, only lower population states had any significant association with Tor search popularity ($p<.05$ in both models). In model 2, for each additional

30,000 people in population size, there was an approximately 0.1% reduction in Tor search popularity – a small magnitude effect. The non-significant relationships with measures like racial composition, education level, and median income while surprising, do *not* indicate that there are no digital inequalities in terms of interest in Tor. Rather, they suggest that any differences that exist are happening at a within-state level, not between-states.

In terms of controls for industry, in model 1, which includes Washington D.C., states with a higher percentage of journalists as share of the work force had significantly higher search popularity for Tor ($p < .05$). For each one percent increase in journalists, there is a 34.2% increase in the popularity of Tor searches. It should be noted that, in all states, journalists account for less than 1% of all employees. Still, this implies a 30% difference in the interest in Tor from the state-year with the fewest journalists to the state-year with the greatest share of journalists. In model 2, where we drop the D.C. cases and control for the political measures, the journalism measure is non-significant. Nonetheless, the coefficient is still positive (suggesting a 13% increase in Tor for each one percent increase in journalists) and, given that these data represent a population of state-years, these findings tend to suggest states with more journalists have greater interest in Tor. The industry measures for the proportion of tech and legislative jobs were not significantly associated with searches for Tor. Likewise, neither of the political measures were significantly associated with Tor search popularity ($p > .05$).

DISCUSSION

The results of this study demonstrate that between 2006 and 2015, interest in Tor as measured by Google search popularity grew substantially in every state. In both models, some of the largest effects were the year dummies (especially for 2011 and 2014), which indicated large increases in interest in Tor over time. The simple time effect accounts for more than either interest in Snowden or in the Dark Web. In a recent interview, Fran Morente said that many news stories had turned the public’s attention to dataveillance briefly, but that “we are still waiting for a cataclysmic Chernobyl-like data earthquake” (Morente and Marx 2019:2). In fact, rather than a one-time explosion, there seems to have robust growth in interest in Tor over time in the US.

Interest in Tor was significantly higher in state-years with greater interest in Edward Snowden, supporting H_1 . In our full model, for every 10% increase in the popularity of searches related to Snowden, there was a 7.4% increase in Tor search popularity. However, we reject H_2 given that interest in the Dark Web was not significantly associated with interest in Tor. Of Tor’s two stories, the anti-surveillance story, rather than the illicit lure of the Dark Web story, appears to be more closely associated with interest in the software.

Drawing on Ball’s (2009) concept of “exposure,” we argued that the Snowden story was an issue-attention cycle that created the social conditions for Americans to feel a stronger sense of exposure to surveillance. In states where the Snowden issue-attention cycle gained greater traction, members of the public may have explored ways of managing their exposure by investigating the “distributed masking move” of using Tor. The results of this study are consistent these claims. However, as one anonymous reviewer pointed out, unlike Downs’ (1972) original

concept of issue-attention *cycles*, what we seem to observe in the case of Snowden is an issue-attention *surge*. Overall interest in Tor has continued to grow over time and in states where Snowden continues to be of interest, we observe higher levels of interest in Tor. For advocates of individual privacy online, these findings indicate that powerful stories about state mass surveillance may produce not only avoidant chilling effects in the public (Marthews and Tucker 2017), but may also inspire an interest in software that allows people to protect themselves. It is unlikely that Edward Snowden himself will ever make such a great media splash again. Nonetheless, activists who aim to raise public awareness of mass surveillance may be heartened by these results.

By contrast, interest in the Dark Web, whether for its cryptomarkets or illegal content, was not strongly associated with Tor. Perhaps, people who search on Google for the “Dark Web” simply have a lurid curiosity about what it is and have no real intention in of acquiring the means of accessing it. Determined Dark Web users may be somewhat more aware of potential exposure to surveillance and, therefore, might avoid searching Google for terms like “Dark Web” and “Tor.” What the results do tend to indicate is that, in state-years where a Dark Web issue-attention cycle has peaked, it does not translate into a massive recruitment drive for Tor. Put differently, access to the Dark Web is a real motivation for some users of Tor, but waves of attention to the Dark Web at the state-level do not appear to be the kind of story that substantially engages the public’s interest in Tor.

Several of the control measures in this study yielded intriguing results that might prompt future lines of inquiry. In one of the models, states with a higher proportion of journalists had significantly higher Tor search popularity. There are legitimate reasons that many journalists might want to use software like Tor to shield their searches and communications from surveillance by states, corporations, and hackers. As previously noted, several major publications have established outposts on the Deep Web, inviting anonymous leaks of newsworthy document. But states with a particularly high share of journalists may differ culturally from other cities in any number of ways. Rather than offering hard proof that journalists are using Tor *en masse*, this finding ought to invite future research to explore the rate and manner of use of anonymity-granting technologies by journalists at the individual-level. By the same token, the non-significant measures of the share of legislative and tech jobs should not be taken as evidence that tech and political workers don’t use Tor. Professionals in these industries may be concerned enough about anonymity that they use an anonymous search engine like DuckDuckGo rather than Google in the first place.

The findings were also potentially surprising because of how many factors were non-significant. There was substantial variation in Tor interest between states, with some states like Wyoming having consistently high interest in Tor and, others, like Louisiana having lower than average search popularity for Tor in all years. Despite some clear differences between states, the variation was not particularly patterned. Interest in Tor is not a red state vs. blue state issue. It is not of interest to people only in coastal urbanized states or in wealthy, highly educated states. Controlling for other factors, lower population states did have significantly higher search popularity for Tor. However, more educated, affluent, younger, more urban, and higher percentage

white states with more home broadband did not have significantly higher search popularity for Tor, despite potentially greater opportunity.

One possibility is that there are, indeed, differences between people who pursue anonymity-granting technologies and those who don't, but they are simply not structured at the state level. The ecological approach of the current study allows us to examine the effects of contextual conditions on the public interest in Tor, but prevents us from observing the enormous heterogeneity within states. Future research ought to address these limitations in two ways. First, research might examine the sociological conditions associated with public interest in Tor using smaller geographic units than states, such as metropolitan areas. If our state analysis conceals some of the sub-state heterogeneity, an analysis at the Metropolitan Statistical Area (MSA) level would offer an opportunity to examine the conditions experienced by people in that city. In the long term, the preferable option would be to have individual-level survey data with a range of questions about attitudes regarding the use of anonymity-granting technology. If large sample surveys, like the General Social Survey and the American National Election Studies incorporate survey questions about the use of anonymity-granting technologies, it would be possible to attach contextual data from the American Community Survey and other sources to conduct multilevel analyses. Such analysis would allow us to distinguish between the individual characteristics and the community level conditions that make interest in anonymity-granting technologies more or less likely.

CONCLUSION

This research is the first to examine the sociological conditions associated with greater public interest in Tor within the U.S. The results offer some indication that issue-attention cycles that increase public interest in state surveillance, such as the Snowden revelations, are associated with greater interest in Tor. This finding may reflect the public's desire to manage their growing sense of exposure to surveillance by adopting a "masking move." Cycles of public interest in the Dark Web show no sign of driving the public to Tor in droves. Additionally, this study finds that interest in Tor bridges liberal and conservative states, affluent and poor states, and states with varying degrees of racial diversity. Though "digital inequalities" certainly exist, this study indicates that variation in interest in anonymity-granting technologies exists within-states rather than between-states. More research at the individual-level is needed to better understand how individuals consider the use of anonymity-granting technology, but this study is among the first to document the link between the Snowden issue-attention cycle and growing public interest in protecting themselves from state surveillance.

REFERENCES

- Ackerman, Spencer, and Sabrina Siddiqui. 2015. "NSA Surveillance Opposed by American Voters from All Parties, Poll Finds." *The Guardian*, May 18. <https://www.theguardian.com/us-news/2015/may/18/us-voters-broadly-opposed-nsa-surveillance>.
- Aldridge, Judith, and David Décary-Hétu. 2014. "Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation." Available at SSRN 2436643.
- Amoore, Louise and Marieke De Goede. 2005. "Governance, risk and dataveillance in the war on terror." *Crime, law and social change*, 43(2-3):149-173.
- Ball, Kirstie. 2009. "Exposure: Exploring the subject of surveillance." *Information, Communication & Society* 12(5):639-657.
- Barratt, Monica J. 2012. "Silk Road: eBay for Drugs." *Addiction* 107(3): 683-683.
- Bancroft, Angus and Peter Scott Reid. 2017. "Challenging the techno-politics of anonymity: the case of cryptomarket users." *Information, Communication & Society* 20(4):497-512.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B J Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8 (2): 121-44.
- Berry, William D, and Evan J Ringquist. 1998. "Measuring Citizen and Government Ideology in the American States , 1960-93." *Political Science* 42 (1): 327-48.
- Bertrand, Natasha. 2015. "ISIS Is Taking Full Advantage of the Darkest Corners of the Internet." *Business Insider*, July 11. <http://www.businessinsider.com/isis-is-using-the-dark-web-2015-7>.
- Chawki, Mohamed. 2010. "Anonymity in Cyberspace: Finding the Balance between Privacy and Security." *International Journal of Technology Transfer and Commercialisation* 9: 183.
- Chertoff, Michael. 2017. "A public policy perspective of the Dark Web." *Journal of Cyber Policy* 2(1):26-38.
- Clarke, Roger. 1988. "Information technology and dataveillance." *Communications of the ACM* 31(5):498-512.
- Davis, Jenny L. and James B. Chouinard. 2016. "Theorizing affordances: From request to refuse." *Bulletin of Science, Technology & Society* 36(4):241-248.
- Degli Esposti, Sara. 2014. "When big data meets dataveillance: The hidden side of analytics." *Surveillance & Society*, 12(2):209-225.
- DiGrazia, Joseph. 2014. "The Tea Party Movement: Right-Wing Mobilization in the Age of Obama." Indiana University.
- . 2015. "Using Internet Search Data to Produce State-Level Measures: The Case of Tea Party Mobilization." *Sociological Methods & Research*, 0049124115610348-.
- Downs, Anthony. 1972. "Up and down with Ecology: The 'Issue-Attention Cycle.'" *Public Interest* 28 (1): 38-50.
- Dupont, Benoit. 2008. "Hacking the panopticon: Distributed online surveillance and resistance."

- In *Surveillance and governance: crime control and beyond*, Volume 10 (pp. 257-278), Mathieu Deflem and Jeffrey T. Ulmer (ed.). Bingley, UK: Emerald Group Publishing Limited.
- French, Lauren, and Kate Tummarello. 2015. "Liberals, Conservatives Unite vs. NSA Spying." *Politico*, May 4. <http://www.politico.com/story/2015/05/liberal-conservatives-nsa-spying-patriot-act-117586>.
- Gehl, Robert W. 2016. "Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network." *new media & society* 18(7):1219-1235.
- Google. 2017. "Google Trends." <https://trends.google.com/>.
- Greenwald, Glenn. 2013. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*, June 6. <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
- Greenwald, Glenn, and Ewen MacAskill. 2013. "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data." *The Guardian*, June 11. <https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>.
- Gros, Valentin, Marieke de Goede, and Beste İşleyen. 2017. "The Snowden Files Made Public: A Material Politics of Contesting Surveillance." *International Political Sociology* 11(1):73–89.
- Gross, Neil, and Marcus Mann. 2017. "Is There a 'Ferguson Effect?' Google Searches, Concern about Police Violence, and Crime in U.S. Cities, 2014 – 2016." *Socius* 3: 1–16.
- Haggerty, Kevin D. and Richard V. Ericson. 2000. "The surveillant assemblage." *The British Journal of Sociology* 51(4):605-622.
- Hargittai, Eszter, and Kaitlin Jennrich. 2016. "The Online Participation Divide." In *The Communication Crisis in America, And How to Fix It*, edited by Mark Lloyd and Lewis A. Friedland, 199–213. New York: Palgrave Macmillan.
- Hills, Jill. 2006. "What's New? War, Censorship and Global Transmission: From the Telegraph to the Internet." *International Communication Gazette* 68 (3): 195–216. doi:10.1177/1748048506063761.
- Jardine, Eric. 2016. "Tor, What Is It Good for? Political Repression and the Use of Online Anonymity-Granting Technologies." *New Media & Society*, 1–18.
- . 2015. "The Dark Web Dilemma: Tor, Anonymity and Online Policing." *Global Commission on Internet Governance Paper Series*, no. 21: 1–13.
- Karni, Annie, and Alex Isenstadt. 2017. "Sean Spicer Targets Own Staff in Leak Crackdown." *Politico*, February 26. <https://www.politico.com/story/2017/02/sean-spicer-targets-own-staff-in-leak-crackdown-235413>.
- Katz, Vikki, Victoria Rideout, Carmen Gonzalez, Alexia Raynal, Michael H. Levine, and Catherine Jhee. 2016. "Opportunity for All?: Technology and Learning in Lower-Income Families." Washington, D.C. <http://digitalequityforlearning.org/>.
- Landau, Susan. 2013. "Making Sense from Snowden : What 's Significant in the NSA Surveillance Revelations." *IEEE Security & Privacy* 13 (July/August): 54–63.

- Lawrence, Dune. 2014. "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built." *Bloomberg Businessweek*.
<https://www.bloomberg.com/news/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency>.
- Loshin, Peter. 2013. *Practical Anonymity: Hiding in Plain Sight Online*. Waltham, MA: Elsevier.
- Lyon, David. 2003. *Surveillance after September 11*. Cambridge, UK: Polity.
- . 2006. "The search for surveillance theories." In *Theorizing Surveillance*, (pp. 17-34), David Lyon (ed). New York: Routledge.
- Lyon, David, Kevin D. Haggerty, and Kirstie Ball. 2012. "Introducing surveillance studies." In *Routledge Handbook of Surveillance Studies* (pp. 33-44), Ball, Kirstie, Kevin D. Haggerty, and David Lyon (ed.). New York: Routledge.
- Maddox, Alexia, Monica J. Barratt, Matthew Allen, and Simon Lenton. 2016. "Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'." *Information, Communication & Society* 19(1):111-126.
- Marthews, Alex, and Catherine Tucker. 2017. "Government Surveillance and Internet Search Behavior." *Social Science Research Network*.
- Marx, Gary T. 2003. "A tack in the shoe: Neutralizing and resisting the new surveillance." *Journal of Social Issues*, 59(2):369-390.
- Marx, Gary T. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.
- Moore, Daniel, and Thomas Rid. 2016. "The Darkness Online: Cryptopolitik and the Darknet." *Global Politics and Strategy* 58 (1): 7–38.
- Murakami Wood, David, and C. William R. Webster. 2009. "Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example." *Journal of Contemporary European Research*, 5(2):259-273.
- Olmstead, Kenneth. 2017. "Most Americans Think the Government Could Be Monitoring Their Phone Calls and Emails." Washington, D.C. <http://www.pewresearch.org/fact-tank/2017/09/27/most-americans-think-the-government-could-be-monitoring-their-phone-calls-and-emails/>.
- Owenson, Gareth and Nick Savage. 2015. "The Tor Dark Net." *Global Commission on Internet Governance Paper Series* 20:1-20.
- Paquet-Clouston, Masarah, David Décary-Héту, and Carlo Morselli. 2018. "Assessing market competition and vendors' size and scope on AlphaBay." *International Journal of Drug Policy* 54:87-98.
- Rainie, Lee and M Madden. 2015. "Americans' Privacy Strategies Post-Snowden." *Pew Research Center*, 1–37.
- Rhumorbarbe, Damien, Ludovic Staehli, Julian Broséus, Quentin Rossy, and Pierre Esseiva. 2016.

- “Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data.” *Forensic Science International* 267:173-182.
- Robinson, Laura. 2014. “Freeways, Detours and Dead Ends: Search Journeys Among Disadvantaged Youth.” *New Media & Society* 16 (2): 234–51.
- Roy, Jessica. 2013. “Feds Raid Online Drug Market Silk Road.” *Time*, October 2. <http://nation.time.com/2013/10/02/alleged-silk-road-proprietor-ross-william-ulbricht-arrested-3-6m-in-bitcoin-seized/>.
- Soska, Kyle and Nicolas Christin. 2015. “Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.” Paper presented at the *24th USENIX Security Symposium* Washington, D.C., August 12-14:33-48.
- Stephens-Davidowitz, Seth. 2014. “The Cost of Racial Animus on a Black Candidate: Evidence Using Google Search Data.” *Journal of Public Economics* 118: 26–40.
- Stout, David. 2006. “Justices Set Limits on Public Employees’ Speech Rights.” *The New York Times*, May 30. <http://www.nytimes.com/2006/05/30/washington/30cnd-scotus.html>.
- van Dijck, José. 2014. “Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology.” *Surveillance & Society*, 12(2):197-208.
- “Who Uses Tor?” 2017. *The Tor Project*. <https://www.torproject.org/about/torusers.html.en>.

FIGURES AND TABLES

Table 1. Descriptive Statistics

Variable	<i>n</i>	Mean	SD	Min	Max
Tor search popularity	510	33.34	11.22	13.32	77.08
Snowden search popularity	510	2.09	3.56	0.00	21.50
Dark web/Deep web/ Silk Road search popularity	510	1.93	1.89	0.00	11.50
% with home web access	510	74.77	7.83	49.48	88.76
Population (in 10,000s)	510	608.50	683.26	51.50	3914.48
Population density (logged)	510	4.59	1.52	0.16	9.31
Median household income	510	55366.89	9180.30	38305.00	77850.43
Gini coefficient (*100)	510	45.70	2.28	40.20	54.20
% white	510	77.24	13.61	24.61	96.25
% under age 35	510	46.88	3.01	39.12	59.59
% with college degree or more	510	28.35	5.86	16.51	56.75
State NOMINATE score	500	47.76	28.34	0.00	92.45
Citizen ideology score	500	52.79	15.74	13.48	93.25
% tech jobs (*100)	510	2.36	1.01	0.75	5.77
% journalism jobs (*100)	510	0.11	0.10	0	0.88
% legislative jobs (*100)	510	0.05	0.04	0	0.19

Figure 1. Google Search Popularity for “Tor” Over Time (2006-2015)

Figure 2. Kernel Density Plots of “Tor” Search Popularity By State

Figure 3. Search Popularity for “Tor” By State-Year

Table 2. Time/State Fixed Effects Regression of Independent Variables on Tor Search Popularity

	(1)	(2)
Population (in 10,000s)	-0.028*	-0.031**
	(0.011)	(0.012)
Pop. density (logged)	4.997	17.391
	(16.400)	(16.729)
Median HH income	-2.37e-5	-3.71e-5
	(2.164e-4)	(2.177e-4)
Gini coefficient (*100)	-0.684	-0.817
	(0.475)	(0.477)
% White	0.033	0.265
	(0.276)	(0.295)
% Under 35	-0.081	0.530
	(0.652)	(0.680)
% College Degree+	-0.636	0.564
	(0.471)	(0.551)
% Home Web Access	0.105	0.051
	(0.131)	(0.131)
% Tech Jobs	2.205	2.359
	(1.714)	(1.727)
% Journalism Jobs	34.208*	13.455
	(15.321)	(17.659)
% Legislative Jobs	0.713	4.720
	(10.947)	(10.903)
Snowden Search Popularity	0.535*	0.745*
	(0.261)	(0.306)
Dark Web Search Popularity	0.591	0.715
	(0.425)	(0.425)
State NOMINATE Score		-0.023
		(0.017)
State Citizen Ideology Score		0.030
		(0.046)
2007	2.970*	2.660*
	(1.153)	(1.198)
2008	3.090*	2.670
	(1.443)	(1.519)
2009	4.287*	3.635*
	(1.788)	(1.801)
2010	4.992*	4.608*
	(2.281)	(2.294)
2011	20.478***	19.740***
	(2.512)	(2.514)
2012	18.000***	16.603***
	(2.973)	(2.976)
2013	15.166***	10.764*
	(3.921)	(4.324)
2014	24.485***	20.788***
	(3.462)	(3.636)

2015	17.665*** (4.221)	13.270** (4.364)
Constant	48.886 (82.692)	-70.899 (87.548)
n	510	500
R^2	0.821	0.829
AIC	2998.467	2928.517
BIC	3095.858	3033.882

* $p < .05$, ** $p < .01$, *** $p < .001$; standard errors in parentheses

ⁱ No consensus exists on the correct terminology to refer to various sectors of the Internet. We use “Deep Web” to refer to portions of the web not indexed by conventional search engines and accessible by standard web browsers. We use “Dark Web” to refer to the portion of the “Deep Web” devoted to illegal activities (e.g., illegal arms sales, drug sales, child abuse imagery sites). However, in other literature, “Dark Web” and “Deep Web” are sometimes used interchangeably.

ⁱⁱ Following DiGrazia (2015), we conducted joint searches with the “Snowden” topic and three random words (e.g. “noodle”). We then conducted a factor analysis and used the resulting factor scores as our estimated measure of “Snowden” searches. Finally, for ease of interpretation, we converted these scores back to the Google Trends’ normalized scale by setting the top estimated value to the peak observed value (21.5) and other values as a proportion of the peak.

ⁱⁱⁱ We conducted a Hausman test to compare the choice of a fixed effects rather than a random effects model. The statistically significant result ($p < .001$) suggests a fixed effects model is preferable because unique state errors are correlated with the regressors. We also conducted a post-estimation test on year effects (*testparm* in Stata 14.2) to see if the dummy variables for all years are equal to 0. Due to the statistically significant result ($p < .001$), we employ time fixed effects as well. Due to reviewer feedback on an earlier version this paper, we also estimated a random intercept model (available upon request), but it did not substantially change the results.

^{iv} VIF for all predictors is less than 10 and condition number for complete model is 7.2.