Journal of
Peace Research

Terrorism and internet censorship

Journal of Peace Research
1–12
© The Author(s) 2020
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0022343320959369
journals.sagepub.com/home/jpr
SAGE

Stephen A Meserve

Department of Politics and International Affairs, Northern Arizona University

Daniel Pemstein

Department of Political Science & Public Policy and Challey Institute for Global Innovation and Growth, North Dakota State University

Abstract

The internet provides a powerful tool to terror organizations, enhancing their public messaging, recruitment ability, and internal communication. In turn, governments have increasingly moved to disrupt terror organizations' internet communications, and even democracies now routinely work to censor terrorist propaganda, and related political messaging, in the name of national security. We argue that *democratic* states respond to terror attacks by increasing internet censorship and broadening their capacity to limit the digital dissemination of information. This article builds on previous work suggesting this relationship, substantially improving measurement and estimation strategy. We use latent variable modeling techniques to create a new measure of internet censorship, cross nationally and over time, from internet firm transparency reports, and compare this measure to an expert-survey based indicator. Leveraging both measures, we use a variety of panel specifications to establish that, in democracies, increases in terror predict surges in digital censorship. Finally, we examine the posited relationship using synthetic control methods in a liberal democracy that experienced a large shock in terror deaths, France, showing that digital censorship ramped up after several large terrorist attacks.

Keywords

internet censorship, latent variable models, terrorism

Introduction

Since a core interest of the state is to protect itself, its agents, and its rule (Tilly, 1990), theories of states' survival interests suggest that governments meet activities that threaten them with repression. A large literature identifies the ways in which digital communications technology facilitates groups that oppose the state by enabling them to recruit, organize, and coordinate action (Tufekci, 2017).[1] In response, governments developed and refined tools to restrict digital communications (Tufekci, 2017; Roberts, 2018) in order to – among other things – protect against terrorism and insurgency.

But how do findings about tools for digital control and repression explain behavior by democratic regimes? Most definitions of democracy rest on a bedrock of freedom of expression, and all measures of democracy demand that governments allow opposition to freely organize, compete, and dissent politically. Democracies may, therefore, abhor digital censorship. The literature provides suggestive but limited answers about democratic digital control (Deibert et al., 2008, 2010; MacKinnon, 2012), but most of what we know about digital content restriction rests on studies of autocracies that are relatively unconstrained with respect to freedom of expression. Do democratic states control digital spaces, or do they maintain free and open communication, in response to threats? To the extent that they do restrict online speech, how do they censor?

[1] These expectations in the digital realm parallel recent theory, measurement, and empirical research on traditional press and media freedom and civil conflict (Whitten-Woodring & Van Belle, 2017).

Corresponding author:
daniel.pemstein@ndsu.edu

We provide evidence that democracies respond to internal threats with repressive and controlling behavior, but they use a different suite of tools than authoritarian regimes. We focus on their use of intermediaries to remove content: treating online content providers as 'points of control' (Zittrain, 2003). We hypothesize that the imperatives of state survival apply to democracies under threat, despite countervailing pressures to protect broad citizen freedoms. Democracies tend to work within legal frameworks to remove digital content. But our empirical picture of what this process looks like is far from complete and understanding democratic digital censorship is fundamental to timely policy debates about who – governments or firms – should be responsible for policing internet content.

While previous work explores associations between terrorism and digital content controls, measurement strategies and findings remain relatively limited, exploring a brief time frame and using a single measure of digital restriction, based on the products of a single company, Google LLC (Meserve & Pemstein, 2018). Here we delve into the topic of digital censorship and security threats in greater depth and specificity, refining the measurement of internet restrictions and demonstrating the robustness of the relationship between digital censorship and terrorism to new data and methods, with a greater attention to causation. We apply panel data and synthetic control techniques to new measures of internet freedom and state digital censorship. We create a new measure of internet censorship, using a latent variable model to scale internet transparency reports from major multinational firms. We also perform tests using new, expert-rated measures of internet freedom, in order to confirm that our firm-based measures produce results that are consistent with a broader, but more subjective, assessment of content regulation.

We find consistent, compelling evidence that violent opposition induces states to censor digital content and reduce internet freedoms. Our data show that restricting digital content and internet freedom, in response to terrorism, is not simply a behavior performed by illiberal regimes like Turkey (Meserve & Pemstein, 2018; Gohdes, 2018). We find that even liberal democracies respond to terrorism and insurgency by tightening content restrictions through the use of legal mechanisms that force a variety of online content providers (OCPs) to censor content on their behalf, rather than relying on the direct infrastructure control and filtering techniques pioneered by countries like China. After presenting our panel data evidence, we examine the case of France, using synthetic control methods to show how sensitive digital freedoms are to security threats to the state. After several deadly terrorist events, France greatly tightened its legal rules on digital content, going so far as to authorize a state of emergency that resulted in a tremendous number of content restrictions and overall reduction in internet freedom. We show that internet freedom in liberal democracies is sensitive to internal threats, and that democratic governments, like their autocratic counterparts, restrict digital freedom when faced with terrorism and insurgency.

Controlling communications on the internet

The spread of digital technology strengthens opposition groups' capacity to organize and act collectively. Digitally networked movements use a variety of tools unavailable to previous generations of social movements and opposition groups. Tufekci (2017) outlines how people use digital tools to help found, organize, and coordinate protest movements ranging from the Arab Spring to Occupy Wall Street. Participation by peripheral, less committed individuals is critical to the success of collective action, and digital tools provide networked movements with the ability to reach and persuade critical fringe individuals to join and act (Barberá et al., 2015; Steinert-Threlkeld, 2017). Oversimplifying, digital technology initially made it easier to reach and network diverse people with similar grievances. Digital networks also make it easier to cross boundaries and evade governments by acting transnationally, pushing issues into and out of different national jurisdictions and facilitating the provision of material support to those in other political environments or regime types (Keck & Sikkink, 1998).

While some literature focuses on democratic opposition groups and protests like the Arab Spring, or the suppression of Turkish opposition, the same tools that facilitate networked protest are also used by violent opposition groups. Digitally empowered domestic and international terrorists, for example, recruit and plan across borders, away from prying government eyes. At the subnational level, access to cell phone networks and social media are associated with more insurgent violence (Warren, 2015), but digital technologies also may facilitate loyal groups collaborating with government forces (Shapiro & Siegel, 2015). The interaction between access to digital tools and government restrictions of internet content even modulates how governments target repression against regime opponents, and how much violence insurgents perpetrate (Gohdes, 2015, 2020; Bak, Sriyai & Meserve, 2018).

Digital content scholars suggest that states facing internal pressures and violent threats reasserted their power over citizen digital communications using what DeNardis (2014: 199) calls 'the dark arts of internet governance'. States played technological and infrastructural catch-up to master systems of digital control in order to combat opposition movements in the early years of the 21st century. While 'the costs to governments of fear-based censorship are more severe in the information age' (Roberts, 2018: 54), after initial missteps, state authorities have pioneered new digital content controls to minimize the damage of networked opposition.

The bulk of the aforementioned literature focuses on authoritarian regimes, where we would expect an unconstrained state response. Authors have explored how authoritarian regimes leverage digital tools like social media to stabilize the regime (Gunitsky, 2015), using it as a form of repression technology (Rød & Weidmann, 2015). The most well-studied example, China, constructed a vast censorship apparatus, which features all manner of coercive control – from human censors, relatively porous blocking of the ability to see outside country content, and the production of a flood of misinformation that makes finding the truth difficult for Chinese citizens (King, Pan & Roberts, 2013; Roberts, 2018). We know, fairly comprehensively, that authoritarian regimes do their best to control digital spaces in response to regime threats.

But democracies are, arguably, substantially more constrained in their ability to control digital spaces. Do the implications of the large literature on digital censorship in autocracies carry over to the democratic space? We provide systematic evidence that democracies do their own kind of filtering, often pressuring multinational firms to censor for them (Deibert et al., 2008, 2010; MacKinnon, 2012). Indeed, 'while billions of people use the internet, a small number of services capture or shape most of their activities' – including protest, mobilization, and organization (Tufekci, 2017: 135). This leads democracies to engage in 'delegation of censorship' to OCPs to control content that endangers the state (Seltzer, 2008). Additionally, firms have limited resources to contest state pressure, often having little financial incentive to fight individual requests to take down content, and, because the process of censorship is off-loaded onto firms, censorship through private points of control exhibits less oversight than 'old-fashioned' censorship (Adler, 2011). OCP-based restrictions are therefore potentially attractive to democracies, as censorship can be codified in legal systems, can be off-loaded financially to firms, and, especially in less liberal democracies, can be manipulated to effect political censorship that would not stand up to strict legal scrutiny (Adler, 2011; Marsden, 2011; Meserve & Pemstein, 2018). We provide robust, systematic evidence that democracies respond to violent opposition by censoring digital content, and do so specifically through private points of control.

Data and methods

We test the above argument using worldwide biannual data from 2009–17. We chose this period for two reasons. First, takedown data become available in the second half of 2009, making analysis of takedowns impossible before 2009. Second, while other (e.g. V-Dem's) measures of internet censorship stretch further back in the past, widespread internet penetration, and especially social media use, is spotty during the first decade of the 2000s. Thus, while we might have pushed back our analysis of this measure to 2008, or, optimistically, 2006, we decided to use the availability of transparency data as our starting point. Because we focus on democracies, we conduct our core analysis on countries classified as democracies by V-Dem's Regimes of the World (RoW) measure (Lührmann, Tannenberg & Lindberg, 2018), although we include non-democracies in some descriptive analyses, presented in this section.

Measuring internet censorship effort

Takedown requests. Increasingly, OCPs have sought to increase perceptions of transparency by releasing (semi) annual takedown request reports, detailing the extent to which firms fielded requests from governments to remove content from their platforms. All requests in this analysis emanate from government executives and judiciaries, including local, regional, and national authorities. Requests are generated by various executive and judicial processes such as legal rulings, military and police requests, or bureaucratic actions. We rely on data from four large multinational content-providing firms: Facebook, Google, Microsoft, and Twitter.[2] Firms vary in their tendency to comply with requests, although all four claim to evaluate requests with respect to local law. Because previous work relying on Google transparency

[2] All of these firms distribute products used widely internationally, critical for the purposes of cross-national analysis. Second, these firms provide the most consistent data in their transparency reports. Third, these specific firms, with the exception of perhaps Twitter, allow us to incorporate a broad bundle of digital products across the areas of search, social media, business, etc. For more details, see our discussion in Online appendix A.

reports alone may reflect the peculiarities of Google's products and global reach, we use latent variable modeling techniques to combine data from all four firms, extending coverage and focusing attention on patterns that are common to all four firms.[3]

Request data. Facebook has published biannual transparency reports since the first half of 2013, and data on takedown requests since the second half of that year (Facebook Incorporated, 2018). These requests cover material that governments flag as violating local law. Facebook reports each request, rather than each piece of content, as a single data point. Google provides biannual transparency reports, starting in the second half of 2009 (Google LLC, 2018). These reports cover formal requests from governments to remove content, based on local law. Each request may reference one or more pieces of content, but repeated requests to remove the same piece of content count as multiple requests. The data do not include removals that Google performs without prompting, such as the removal of child pornography, and excludes requests to remove intellectual property that are not the result of a court case – that is, Google has another system designed to field and arbitrate such requests directly from firms. Microsoft has released biannual content removal request reports since 2015 (Microsoft Corporation, 2018). Like Facebook and Google, data reflect requests, rather that content items flagged. Microsoft's reports focus specifically on requests initiated by governments. Finally, Twitter provides biannual data on government-initiated requests, starting in 2012 (Twitter Incorporated, 2018). As a consequence, the takedown data are biannual country-level observations of the number of takedown requests for each firm. In the next section, we scale together firm observations to arrive at a latent measure of biannual country content removal effort.

Latent content removal effort. Given the difference in product portfolios and global market share across firms, simply summing up content removal requests across reports is likely to lead to erroneous conclusions. In other words, five Google takedown requests do not equate to five Facebook requests. Reliable cross-national and temporal market share data are also difficult to obtain, limiting our ability to weight contributions by market share. Nonetheless, to average over firm idiosyncrasies, and to leverage all the information available to us, it makes sense to create a composite measure from all four reports. To achieve this goal we treat requests as observable manifestations of underlying effort expended by governments to remove content from the internet, and use Bayesian factor analysis to estimate this latent variable from the firms' transparency reports.

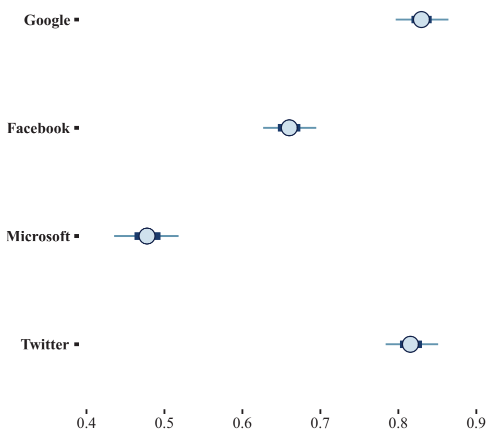


Figure 1. Takedown request factor loadings

We use a simple one-dimensional model.[4] Section D, in the Online appendix, provides information about model specification, estimation, and diagnostics. Figure 1 displays factor loadings, with 95% (thin line) and 50% (thick line) credible intervals and around posterior means. As expected, all four series of takedown requests load positively on the latent trait. Notably, Google and Twitter takedown requests load most highly on the trait, with factor loadings above 0.8, Microsoft requests are more moderately associated with the latent trait with a loading just below 0.5, while Facebook requests fall somewhere in between, approaching 0.7. With the possible exception of the Microsoft loading, factor analysis folk wisdom would classify all of these loadings as 'strong', providing evidence that takedown requests reflect a consistent latent process across firms. Microsoft's somewhat weaker loading may reflect its relatively smaller market share in the social media and content provision spaces, and its limited time coverage.

Figure 2 provides time-series plots for six countries, displaying logged takedown request counts and the latent score across the observation period. We can see that the latent scores track broad trends in the request counts, while smoothing over volatility in the individual scores. They also allow one to take advantage of the longstanding Google data while incorporating information

[3] We discuss takedown requests in more conceptual detail in Online appendix section B.

[4] Exploratory two-dimensional analyses provided little evidence for two latent dimensions.

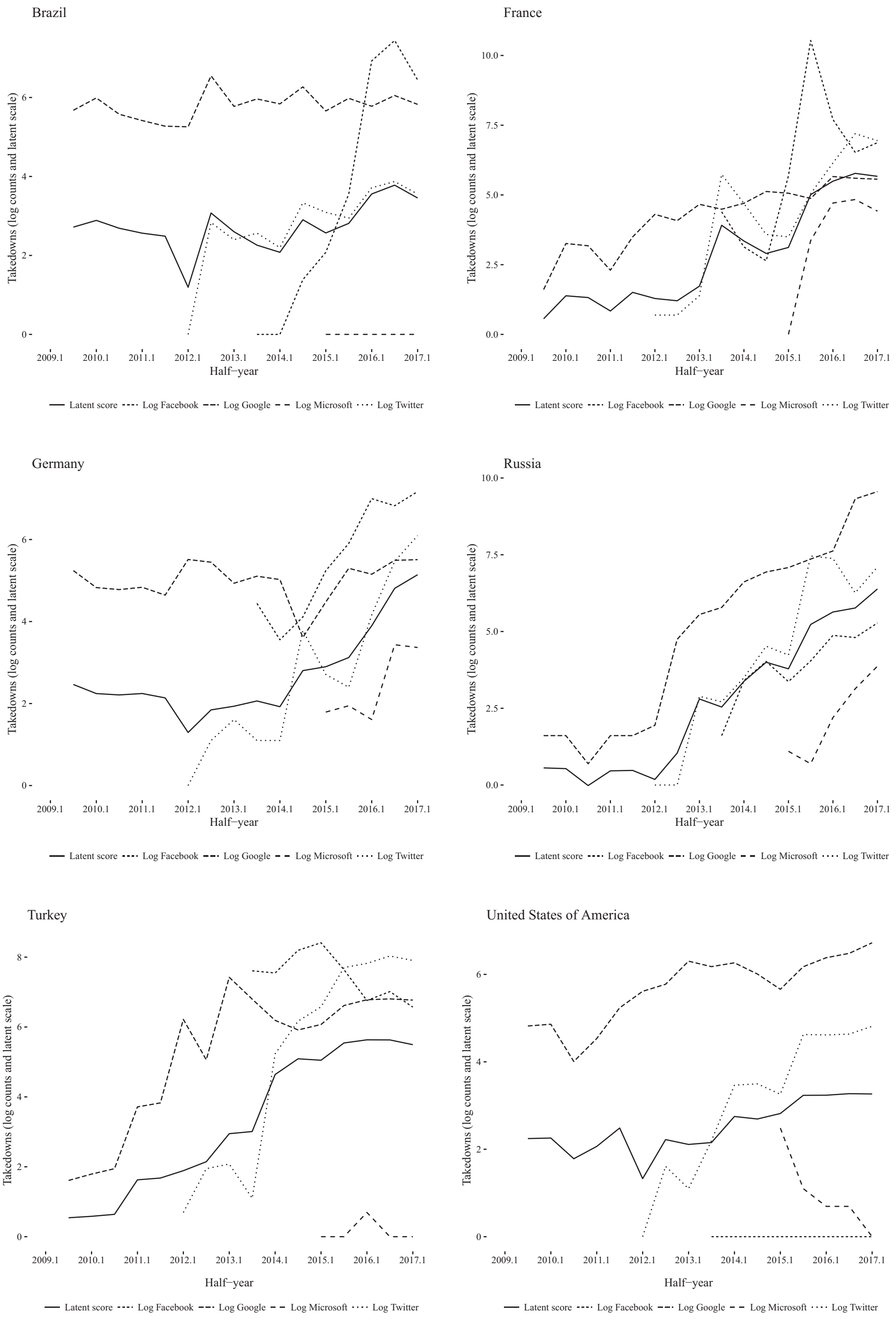


Figure 2. Time-series plots of logged takedown requests and latent takedown scores for six countries

from the other providers as they become available. The figure also highlights the dearth of Microsoft data, which only become available in 2015. This short time series may help to explain the lower loading shown in Figure 1.

Internet censorship effort. While takedown requests provide observable information about government efforts at internet censorship, they are an imperfect measure of political censorship, both because they capture

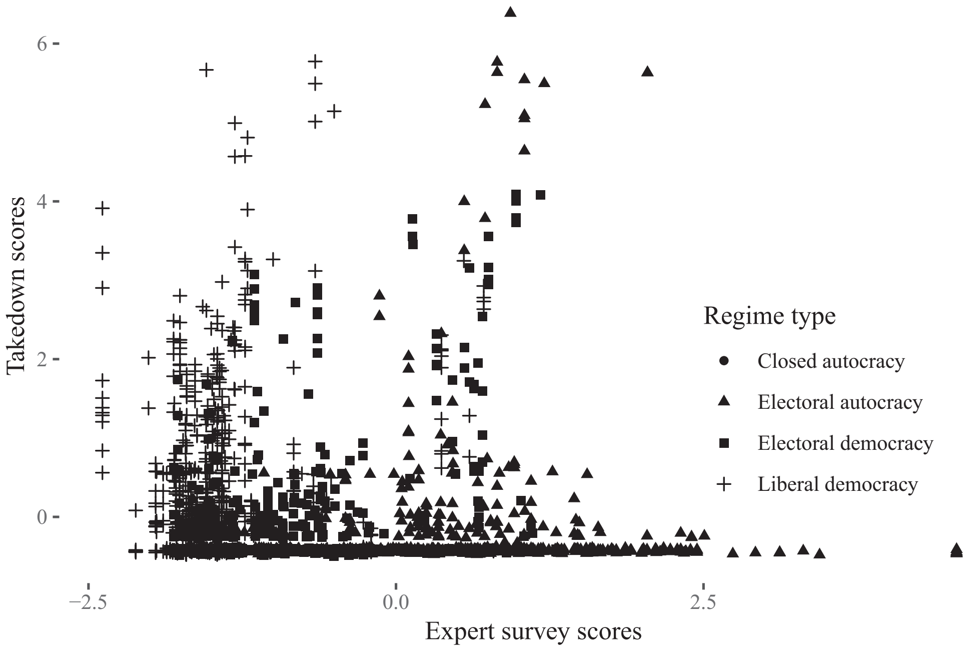


Figure 3. Expert scores and takedown requests

significant non-political censorship, since only a handful of firms provide takedown request reports, and because takedowns capture only one mechanism through which governments censor digital content. We therefore make use of an alternative measure of this latent concept, based on an expert survey fielded by the Varieties of Democracy project (V-Dem). We use a question about government censorship effort (Coppedge et al., 2018; Pemstein et al., 2018) that asked roughly five experts (per observation) to rate country-years on the effort and success government officials have in blocking internet content. For the exact survey question wording, clarification information, and measurement decisions, see Online appendix section C.

Comparing latent internet censorship measures. These two approaches to measuring internet censorship – constructing a latent measure from reported takedown requests, and leveraging subjective ratings – are potentially complementary. They tap different strategies for measuring the censoring of digital content. One is based on objective counts of reported events, while the other leverages subjective evaluations of topic and country experts. The question of which of these measures is more valid is, however, debatable, so we include both in our analysis. The takedown approach measures cross-nationally comparable behavior, reported by a third party without any ulterior interest in obscuring censorship practices. From this perspective, we believe that the takedown-based measure represents a valid, sensitive, behavioral measure of the intensity of censorship. It also focuses on censorship through private points of control, which is the core quantity of interest for our analysis. A potential worry, however, is that some countries do not use private points of control, or use other censorship strategies more intensively. The V-Dem measure captures the subjective perception of experts about censorship within countries. This has the distinct drawback of not measuring actual behavior. On the other hand, this measure allows us to test whether the conclusions drawn from our behavioral analyses have generality, since the subjective assessments by experts will, in principle, capture both the behavior that we focus on here and other forms of censorship.

The two measures are largely uncorrelated ($r = -0.08$). Figure 3 is a scatter-plot of the two scores, broken down by regime type. Clearly, not all countries take advantage of takedown requests. In particular, closed autocracies do not bother with takedowns, likely relying on more forceful measures, and are absent from our data. Electoral autocracies exhibit a non-linear relationship. The raw correlation between measures in this subset is 0.05, but takedown effort can be quite intense among electoral autocracies with expert scores in the 0 to 1 range, while it is rare in electoral autocracies with especially high or low expert censorship scores. If we lump democracies together, we find a correlation of 0.06, but correlations of 0.27 and 0.15 emerge in electoral and liberal democracies, respectively.

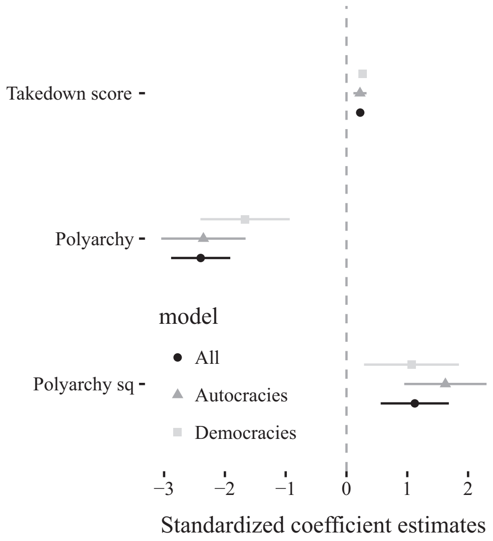


Figure 4. Predicting expert scores with takedown scores

Figure 4 plots coefficients from three models in which we regress expert scores on takedown scores, V-Dem's polyarchy measure (Teorell et al., 2019)[5] and its square, and country fixed effects, for the entire dataset, autocracies, and democracies, as classified by RoW. In each case we find small, but positive, and highly statistically significant ($t > 10$) relationships between our two measures of internet censorship effort. While our two measures capture distinct aspects of the internet censorship, we find that, across the democracy range, takedown request effort predicts expert assessments of censorship effort. The V-Dem measure likely captures a broader range of censorship activities, but takedowns are a good predictor of *digital* censorship scores once we control for the broad package of civil liberties baked into the polyarchy measure.

Independent variables

Key predictors. We measure our key independent variable, *Terrorism*, as the logged total number of terrorist events – and alternatively, as a robustness check, the logged total of deaths caused by terrorist events – in each half-year, reported in the Global Terrorism Database (National Consortium for the Study of Terrorism and Reponses to Terrorism (START), 2018). We also include an alternative indicator, the World Governance Indicator's (WGI) Political Stability and Absence of Violence index (Kaufmann, Kraay & Mastruzzi, 2013). While our primary focus is on the relationship between terrorism and internet censorship, we include this predictor in alternative specifications to test the more general relationship between internal unrest and digital repression.

Covariates. We include a number of covariates to adjust for potential omitted variable bias. First, countries that produce substantial intellectual property (IP) are likely to police content more aggressively than their counterparts and may also face more terrorism. We use population, drawn from the World Development Indicators (WDI), via the Quality of Governance (QoG) dataset (World Bank, 2018; Teorell et al., 2018), to create a *Patents per capita* measure. Similarly, we use the World Intellectual Property Organization's IP filing database (World Intellectual Property Organization, 2018) to measure the number of patent applications originating from each state in the dataset across the time period. *Economic development* predicts internet use, and therefore, likely digital censorship, and potentially terrorism. We therefore include *GDP*, again from the WDI, via QoG. Because more efficient states are more likely to be able to effectively leverage private points of control to censor, we include a measure of *Bureaucratic efficiency* – the number of days it takes to start a business, again from the WDI – in our specifications. We use the WDI's measure of the percentage of *Citizens who regularly use the internet* to capture the importance of digital platforms and use V-Dem's *Polyarchy* variable to control for level of democracy, both of which may causally relate to both terrorism and censorship. Section E in the Online appendix contains summary statistics of our data, for both the full sample and for the sample of democracies.

Estimation

We examine the relationship between terrorism – and internal unrest – and internet censorship in two ways. First, we use panel data techniques to examine the extent to which terrorism and internal unrest predict changes in both takedown requests and expert assessments of governments' internet censorship efforts. Specifically, we use two-way fixed effects models, controlling for country and year. We include the above-described battery of covariates in these models. In particular, trends in internet penetration might plausibly covary with both terrorism and takedown requests, violating the parallel trends assumption inherent in fixed effects regression. Finally,

[5] This is a continuous measure of electoral democracy, ranging between 0 and 1. The ordinal RoW measure that we use to divide the dataset is based on this measure.

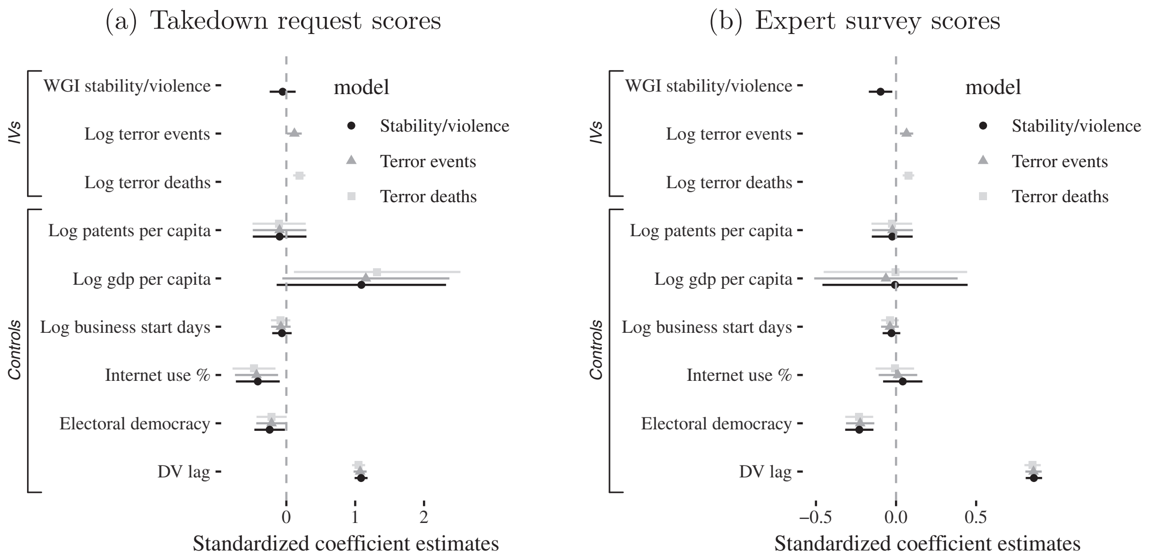


Figure 5. Two-way fixed effect regression coefficients

we include lagged dependent variables to help account for endogeneity.[6]

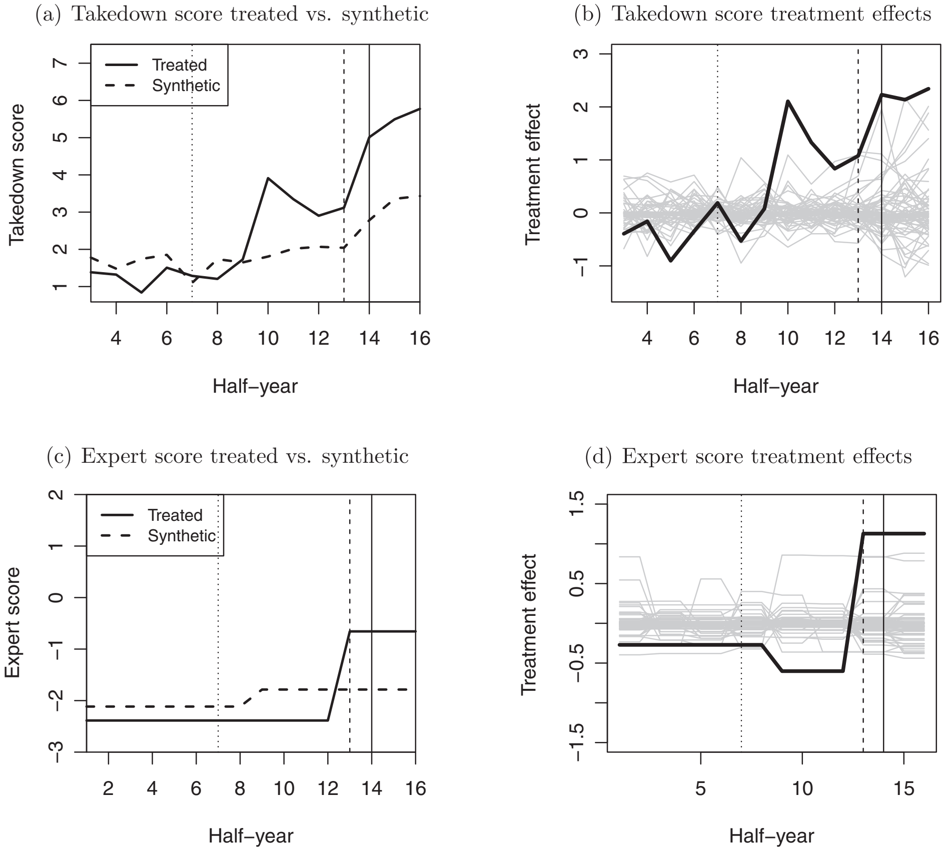
Second, sacrificing generality, but addressing the parallel trends assumption in the fixed effects models, we present a short case study of terrorism and internet censorship in France, and use synthetic control techniques to demonstrate that France significantly increased internet censorship efforts after experiencing a wave of large terrorist incidents. We chose France because it experienced the largest terrorist incident – measured by deaths – of any liberal democracy – measured using V-Dem's RoW indicator – in our sample period. We apply synthetic control techniques (Abadie, Diamond & Hainmueller, 2010) to both of our dependent variables. We include all of the above-mentioned independent variables, and lags of our dependent variables, as predictors when generating synthetic matches.

Results

Figure 5 displays coefficient estimates from two sets of two-way fixed effects regression models of internet censorship effort – measured with (a) takedown scores and (b) expert scores – on three measures of terrorism or internal unrest, a battery of controls, and a lagged dependent variable. We replicate an initial finding from Meserve & Pemstein (2018) that democracies that experience terror censor the internet more aggressively. While previous research relied on a short panel of Google takedown requests, we find this effect across both multifirm takedown scores and expert-based measures. While the standardized coefficients are reasonably small, the effects are, nonetheless, substantively significant. For example, a 30-terror-death half-year is associated with an increase in takedown effort of one-quarter of a standard deviation, and about one-fifth of a standard deviation increase in expert-rated censorship effort.

The effect holds whether we measure terrorism as event counts or deaths. We also use more robust estimation techniques. The original finding was based on a random-effects regression with no lagged dependent variable. Here, leveraging our longer panel, we include fixed effects for country and year, and a lagged dependent variable (and, in the Online appendix, bounding specifications using only fixed effects or lagged DV). The WGI stability and violence index also predicts expert and takedown scores in the expected directions but statistical significance is sensitive to specification (see footnote 6). In sum, we find robust evidence that democracies increase digital repression in response to terrorism, and

[6] Putting a lagged DV in a fixed effects regression can induce bias. The Online appendix reports results of separate fixed effects and lagged dependent variables models, in Tables VI and VII, plausibly placing bounds on effect sizes (Angrist & Pischke, 2009). The direction and statistical significance of our key coefficients are largely robust to specification. The one exception is that the relationship between WGI S&V and takedown scores is statistically insignificant in the combined and fixed effects models, but statistically significant in the ldv-only model, while the relationship between WGI S&V and the latent score is statistically significant in the combined and fixed effects models, but statistically insignificant in the ldv-only model. The WGI S&V coefficient is negative in all models.


(a) Takedown score treated vs. synthetic

(b) Takedown score treatment effects

(c) Expert score treated vs. synthetic

(d) Expert score treatment effects

Figure 6. Synthetic control method, France

Vertical lines denote attacks: Montauban/Toulouse [dotted], Charlie Hebdo [dashed], and Nice [solid]. We treat the pre-Hebdo period (half-years 1–12) as pre-treatment.

some evidence that they do so in response to instability, more generally. This suggests that the liberality of digital freedom is not a given in even the most democratic countries, but instead is, in part, conditional on the existence of internal and external threats to the government.

France

While the panel results establish a general relationship between terrorism and digital censorship, studies of cases that experienced terrorism shocks can help to better establish the plausibility of a causal relationship between terrorism and digital censorship. Meserve & Pemstein (2018) use synthetic control techniques to show that Turkey greatly increased its use of Google takedown requests after a spike in attacks by the Kurdistan Workers' Party (PKK) and the Gezi Park protests. Turkey was, arguably, an electoral democracy at the time, and these events presaged a rapid period of autocratization. Here, we examine a second, perhaps more worrying case. In particular, we focus on *liberal* democracies, again as indicated by V-Dem's RoW measure, and examine the case within this set, France, that experienced the largest terrorist attack, as measured by deaths, during our observation period. France experienced three half-years – half-years 13 and 14 in 2015 and half-year 16 in 2016 – with deaths from terrorist attacks exceeding two standard deviations above the liberal democracy average. These include the Charlie Hebdo attack in January 2015, the Paris attacks in November 2015 (the largest attack on a liberal democracy in the dataset), and the Nice attack in July 2016. The latter two attacks represent the highest casualty incidents among liberal democracies in our dataset.

Figure 6 provides the results of a synthetic control analysis of the French case. Panels (a) and (b) present patterns in takedown scores, while panels (c) and (d) examine expert scores. The left-hand panels (a and c) compare France to a synthetic control case, while the right-hand panels (b and d) plot treatment effects for France (thick black line) and placebos constructed from every other democracy in the dataset. Each graph includes three vertical lines. The first line indicates the 7th half-year (early 2012), when a single gunman killed seven people, over two days, in Montauban and Toulouse. While this time period did not exhibit a particularly high overall count of terrorism deaths, the protracted nature of the event produced substantial news coverage, and this event arguably kicked off a period of heightened awareness of terrorism in France. The second two lines, in half-years 13 and 14, demarcate the Charlie Hebdo and Paris attacks. The Nice attack occurred in half-year 16. We take half-year 13, the Charlie Hebdo attack, as our treatment initiation period when generating synthetic controls.

Looking first at panel (a), we see that takedown rates in France look similar to the control case until the tenth period, when they spike briefly. They then taper back towards the control before jumping dramatically in the period following the Charlie Hebdo attack, and growing after half-year 14. In panel (b) we can see that none of the placebo cases exhibits as large an estimated treatment effect as France. Turning to the bottom panels, panel (c) shows a close correspondence between France and the control case, until half-year 13, when experts report a substantial increase in France's censorship effort.[7] France jumps three full standard deviations – among democracies – on V-Dem's internet censorship measure. Mirroring the results for takedowns, no other case exhibits as large a treatment effect, if we consider Charlie Hebdo, or the Paris attacks, as the treatment period.

Taken together, our synthetic control analyses highlight the extent to which the Charlie Hebdo and Paris attacks triggered a period of heightened censorship in France. The placebo tests, depicted in panels (b) and (d), show that this correspondence between terror and censorship is unlikely to be a matter of chance. At the same time, for both dependent variables, the quality of our synthetic controls leaves a bit to be desired. France exhibits a more volatile takedown trajectory in the pre-Hebdo period than the control, and diverges substantially from it in half-year 10. The pre-treatment period match for the expert measure is more clean, although France exhibits a negative gap in the half-years 9–12. Nonetheless, the magnitude of the treatment effect dwarfs this pre-treatment gap, and the analysis, as a whole, is largely consistent with a substantial and unusual increase in censorship in the wake of the Hebdo and Paris attacks.

Conclusion

Our results indicate that even the most liberal, consolidated democracies respond to terrorism and internal threat by clamping down on the freedom of digital spaces. In contrast to existing literature showing this behavior in autocracies, our evidence comes from states which have fundamental protections for civil liberties. In practice, terrorists and insurgent groups may accomplish some of their goals of shaking the liberal norms of democracies in the digital sphere, forcing regimes to tighten their control over internet speech because of its potential for recruiting, organizing, and coordinating dangerous activities. We show that, measured in multiple ways, and using panel techniques that demand a lot of the data, there is a robust relationship between violence and digital censorship and control. While earlier work has highlighted this mechanism of censorship within democracies (Deibert et al., 2008, 2010), and provided some initial tests (Meserve & Pemstein, 2018), our findings provide substantial evidence of the generality and robustness of this argument. Further, our synthetic control study of France demonstrates our proposed mechanism in action, and shows how major terror shocks can cause liberal democracies to inhibit digital freedoms.

Whether our article represents a normatively disappointing finding depends on one's perspective about the inherent normative 'bad' of digital censorship itself. To an early web crusader, who imagined digital spaces as a neutral new frontier where individuals were reasonably free of state control, it is anathema that even the most liberal democracies will monitor and control internet speech between citizens. Yet, it is important to note that when regimes tighten their control over digital spaces, it is not necessarily the case that this control is done unlawfully or illegitimately. Indeed, in the liberal democracies our models describe, such as France, tightened digital control may be performed at the behest of elected officials, using institutionally provided powers, with relatively broad public approval. What our results suggest is that even democracies' digital spaces are subject to the state and its security interests when governments are threatened. Building content regulation regimes that balance state security interests and freedom to communicate online is already becoming a significant political flash point in democratic (and authoritarian) politics, just as

[7] V-Dem data are yearly, so this jump probably reflects the second half of the year, when France instituted a state of emergency in the wake of the Paris attacks. The half-yearly takedown data spike in half-year 14, consistent with this interpretation.

the balance between security and media freedom was before it, in the 19th and 20th centuries.

Replication data

The dataset, codebook, and code for the empirical analysis in this article, as well as the Online appendix, are available at http://www.prio.org/jpr/datasets.

Acknowledgements

The authors would like to thank Chris Fariss and James Lo for editing this special issue and our reviewers for helpful feedback.

Funding

This research was supported, in part, by a Google Faculty Research Award.

ORCID iD

Daniel Pemstein https://orcid.org/0000-0002-1144-6337

References

Abadie, Alberto; Alexis Diamond & Jens Hainmueller (2010) Synthetic control methods for comparative case studies: Estimating the effect of California's tobacco control program. *Journal of the American Statistical Association* 105(490): 493–505.

Adler, Julie (2011) The public's burden in the digital age: Pressures on intermediaries and the privatization of internet censorship. *Journal of Law and Policy* 20(1): 231–266.

Angrist, Joshua David & Jörn-Steffen Pischke (2009) *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton, NJ: Princeton University Press.

Bak, Daehee; Surachanee Sriyai & Stephen Meserve (2018) The internet and state repression: A cross-national analysis of the limits of digital constraint. *Journal of Human Rights* 17(5): 642–659.

Barberá, Pablo; Ning Wang, Richard Bonneau, John T Jost, Jonathan Nagler, Joshua Tucker & Sandra González-Bailón (2015) The critical periphery in the growth of social protests. *PLOS One* 10(11).

Coppedge, Michael; John Gerring, Carl Henrik Knutsen, Staffan I Lindberg, Svend-Erik Skaaning, Jan Teorell, David Altman, Michael Bernhard, Agnes Cornell, M Steven Fish, Haakon Gjerløw, Adam Glynn, Allen Hicken, Joshua Krusell, Anna Luhrmann, Kyle Marquardt, Kelly McMann, Valeriya Mechkova, Olin Moa, Pamela Paxton, Daniel Pemstein, Brigitte Seim, Rachel Sigman, Jeffrey Staton, Aksel Sundstrom, Eitan Tzelgov, Luca Uberti, Yi-ting Wang, Tore Wig & Daniel Ziblatt (2018) Varieties of Democracy Codebook v8. Technical report. Varieties of Democracy Project: Project Documentation Paper Series.

Deibert, Ronald; John Palfrey, Rafal Rohozinski & Jonathan Zittrain (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, Ronald; John Palfrey, Rafal Rohozinski & Jonathan Zittrain (2010) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

DeNardis, Laura (2014) *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Facebook Incorporated (2018) *Transparency Report: Content Restrictions Based on Local Law*.

Gohdes, Anita R (2015) Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research* 52(3): 352–367.

Gohdes, Anita R (2018) The relationship between state and corporate censorship. *APSA Comparative Politics Newsletter* 18(2): 31–38.

Gohdes, Anita R (2020) Repression technology: Internet accessibility and state violence. *American Journal of Political Science* 64(3): 488–503.

Google LLC (2018) *Transparency Report: Government Requests to Remove Content*.

Gunitsky, Seva (2015) Corrupting the cyber-commons: Social media as a tool of authoritarian stability. *Perspectives on Politics* 13(1): 42–54.

Kaufmann, Daniel; Aart Kraay & Massimo Mastruzzi (2013) World governance indicators.

Keck, Margaret E & Kathryn Sikkink (1998) *Activists Beyond Borders*. Ithaca, NY: Cornell University Press.

King, Gary; Jennifer Pan & Margaret E Roberts (2013) How censorship in China allows government criticism but silences collective expression. *American Political Science Review* 107(02): 326–343.

Lührmann, Anna; Marcus Tannenberg & Staffan I Lindberg (2018) Regimes of the World (RoW): Opening new avenues for the comparative study of political regimes. *Politics and Governance* 6(1): 60–77.

MacKinnon, Rebecca (2012) *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Marsden, Christopher T (2011) *Internet Co-Regulation: European Law, Regulatory Governance, and Legitimacy in Cyberspace*. Cambridge: Cambridge University Press.

Meserve, Stephen A & Daniel Pemstein (2018) Google politics: The political determinants of internet censorship in democracies. *Political Science Research & Methods* 6(2): 245–263.

Microsoft Corporation (2018) *Content Removal Request Report*.

National Consortium for the Study of Terrorism and Reponses to Terrorism (START) (2018) Global terrorism database, data file (http://www.start.umd.edu/gtd, last accessed 30 November 2018).

Pemstein, Daniel; Kyle L Marquardt, Eitan Tzelgov, Yi-ting Wang, Joshua Krussell & Farhad Miri (2018) The V-Dem measurement model: Latent variable analysis for cross-national and cross-temporal expert-coded data. Varieties of Democracy Institute Working paper 21(3rd edition).

Roberts, Margaret E (2018) *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton, NJ: Princeton University Press.

Rød, Espen Geelmuyden & Nils B Weidmann (2015) Empowering activists or autocrats? The internet in authoritarian regimes. *Journal of Peace Research* 52(3): 338–351.

Seltzer, Wendy (2008) The politics of internet control and delegated censorship.

Shapiro, Jacob N & David A Siegel (2015) Coordination and security: How mobile communications affect security. *Journal of Peace Research* 52(3): 312–322.

Steinert-Threlkeld, Zachary (2017) Spontaneous collective action: Peripheral mobilization during the Arab Spring. *American Political Science Review* 111(2): 379–403.

Teorell, Jan; Michael Coppedge, Staffan Lindberg & Svend-Erik Skaaning (2019) Measuring polyarchy across the globe, 1900–2017. *Studies in Comparative International Development* 54(1): 71–95.

Teorell, Jan; Stefan Dahlberg, Sören Holmberg, Bo Rothstein, Natalia Alvarado Pachon & Richard Svensson (2018) The quality of government standard dataset, version jan18.

Tilly, Charles (1990) *Coercion, Capital, and European States 990–1990*. Cambridge: Blackwell.

Tufekci, Zeynep (2017) *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven, CT: Yale University Press.

Twitter Incorporated (2018) *Transparency Report: Removal Requests*.

Warren, T Camber (2015) Explosive connections? Mass media, social media, and the geography of collective violence in African states. *Journal of Peace Research* 52(3): 297–311.

Whitten-Woodring, Jenifer & Douglas A Van Belle (2017) The correlates of media freedom: An introduction of the global media freedom dataset. *Political Science Research and Methods* 5(1): 179–188.

World Bank (2018) World development indicators.

World Intellectual Property Organization (2018) IP Statistics Data Center (http://https://www3.wipo.int/ipstats/).

Zittrain, Jonathan (2003) Internet points of control. *Boston College Law Review* 44(2): 653–688.

STEPHEN A MESERVE, b. 1981, PhD (University of Illinois, 2011); Assistant Professor, Northern Arizona University.

DANIEL PEMSTEIN, b. 1980, PhD (University of Illinois, 2010); Associate Professor, North Dakota State University.