Dec 12th, 12:00 AM

Is the Repeal of Net Neutrality a Necessary Evil? An Empirical Analysis of Net Neutrality and Cybercrime

Doehun Kim
Korea Advanced Institute of Science and Technology, doehun.kim@kaist.ac.kr

Jiyong Park
University of North Carolina at Greensboro, jiyong.park@uncg.edu

Is the Repeal of Net Neutrality a Necessary Evil? An Empirical Analysis of Net Neutrality and Cybercrime

Completed Research Paper

Doehun Kim
KAIST College of Business
291 Daehak-ro, Yuseong-gu, Daejeon 34141, Korea
doehun.kim@kaist.ac.kr

Jiyong Park
University of North Carolina at Greensboro
516 Stirling Street, Greensboro, North Carolina 27412, USA
jiyong.park@uncg.edu

Abstract

While net neutrality guarantees equal access to the Internet and online content, it serves as a limiting factor in identifying and tracking criminal activities in cyberspace by ensuring that data packet is transmitted with equal priority, irrespective of its source and content. Exploiting a natural experiment in which net neutrality policies were officially repealed in 2018 in the United States, this study examines the impact of net neutrality on the occurrence of cybercrime. Our findings suggest that the repeal of net neutrality is negatively associated with the occurrence of malicious code and content in an attempt to compromise computer systems (e.g., malware and ransomware). In contrast, we do not find any significant relationship with cybercrime victimization, and cybercrime that may subsequently occur in compromised systems (e.g., data breaches and denial-of-service attacks). This study provides novel insights into the role of net neutrality and open Internet toward the preventive cybersecurity paradigm.

Keywords: Net Neutrality, Cybercrime, Cybersecurity, Internet Service Provider, Internet Governance, Network Management

Introduction

The Internet has penetrated rapidly into our lives, affecting people's lives (Hoffman et al. 2004), businesses (Forman 2005), the economy (Manyika and Roxburgh 2011), and social and political engagement (Zhuravskaya et al. 2020). From the beginning, the Internet, as a public good, stands for the democratic ethos of fairness and openness. In keeping with these premises, the Federal Communications Commission (FCC) of the United States (US) approved the Open Internet Order in 2010 to preserve the Internet as open, fair, and free, also known as net neutrality (Genachowski 2010). In support of the open Internet, net neutrality has been widely adopted across the globe to guarantee that all data packets will be transmitted with equal priority, irrespective of their source, destination, and content (Nguyen et al. 2020). However, in December 2017, the US FCC officially declared a repeal of net neutrality policies, which sparked controversies and debates regarding the role of net neutrality in data privacy, anonymity, and cybersecurity.

Given that net neutrality has significant implications on privacy (Ohm 2010), the repeal of net neutrality has raised concerns about online privacy and the potential discriminatory behavior of internet service providers (ISPs) against users (e.g., Walsh 2017). The repeal of net neutrality means bypassing the principles of the open Internet, such as no blocking, no throttling, and no paid prioritization, allowing ISPs to block web traffics or impose limits on Internet users. ISPs can inspect, restrict, and control data packets and online content, raising concerns about data privacy and anonymity, which have been considered important for ensuring democracy and freedom of expression in cyberspace (Schwartz 1999). In this regard, companies that support online anonymity and privacy by providing a virtual private network continue to support the principle of net neutrality (Hadley 2018).

In contrast, while net neutrality guarantees equal access to the Internet and online content, it also serves as a limiting factor in identifying and tracking criminal activities in cyberspace. Cybercrime is one of the most serious societal challenges (Hyman 2013). Global cybercrime damage is expected to reach up to $10.5 trillion yearly by 2025 (Steve 2020), and the monthly amount of reported occurrence of malicious content, ransomware, and transactions per month in 2021 was estimated to be $102.3 million on average (Chuck 2021). One of the challenges in tackling cybercrime is identifying the sources and origins of criminals in cyberspace, possibly owing to the inability and unwillingness of ISPs to monitor data packets without appropriate search warrants (Akdeniz 2002; UNODC 2019). Cybercriminals often use proxy servers and hidden services via darknets, such as the Onion Router (Tor), to hide their identities (Chan et al. 2019a). The conflict between openness/anonymity and security has been at the center of the discourse on Internet policies (Kling et al. 1999), innovations leveraging the Internet (Goel 2015), and cybersecurity (Cerf 2022).

ISPs, as online content deliverers and information intermediaries, have been urged to prevent cybercrime and malicious content dissemination (Lee et al. 2018; Rowe et al. 2009). However, they face economic and legal barriers to implementing security technologies when providing users with online content (Hartmann and Giles 2018; Rowe et al. 2009). Therefore, potential cybercriminals may abuse the principle of net neutrality and hide behind the cloak of anonymity on the Internet. Although net neutrality has been considered the central tenet of the open Internet, advocating anonymity and freedom of expression (Bauer and Obar 2014), little attention has been paid to the implications of net neutrality and open Internet on cybercrime and cybersecurity. Prior studies have focused mostly on the economic implications of net neutrality on ISPs and content providers (CPs) (Economides and Tåg 2012; Guo et al. 2017). Hence, this study aims to fill this gap in the literature and shed new light on the role of net neutrality in reshaping cybercriminal patterns, with a particular focus on its origins.

Drawing upon the economics of cybersecurity and criminal acts, we postulate mechanisms by which the repeal of net neutrality that gives authorities to ISPs to control data packets can (i) increase the likelihood of malicious code and content transmission being detected and blocked and (ii) deter criminal conduct by increasing the probability of arrest of potential cybercrime offenders. Considering the role of ISPs in intervening Internet traffic flowing into and out of their networks that the repeal of net neutrality could alter, we classify types of cybercrime based on the medium through which it can occur, in the interest of substantiating the link between net neutrality and cybercrime occurrence.

In the US, the repeal of net neutrality took effect in June 2018 across the country (Jamison 2018). However, not all states have approved the repeal of net neutrality, and some states denied federal legislation by introducing state-level legislation to maintain net neutrality. Thus, the state-specific responses to the

repeal of net neutrality policies set up a natural experiment in which the treatment group includes states that supported the FCC's decision (i.e., net neutrality was repealed in 2018). The control group includes states that implemented or initiated their own rules to support net neutrality, and thereby, net neutrality has been in place even after 2018. To measure cybercrime occurrence at the state level, we use data from the Internet Crime Complaint Center (IC3), which provides the number of perpetrators and victims for various types of Internet-related crimes. Upon constructing panel data for 51 states (including the District of Columbia) in the US from 2016 to 2020, we identify the impact of the repeal of net neutrality on the number of cybercrime occurrences using the difference-in-differences (DID) model.

Our findings suggest that the repeal of net neutrality is negatively associated with the occurrence of malicious code and content in an attempt to compromise computer systems (e.g., malware and ransomware). In contrast, we do not find any significant relationship with cybercrime victimization, which implies that the repeal of net neutrality plays a role in preventing cybercrime from occurring or being transmitted from origins rather than protecting users. Additionally, the repeal of net neutrality is found to have insignificant effects on cybercrime that may subsequently occur in compromised systems (i.e., malicious attacks and access). It is also found that the repeal of net neutrality does not influence general Internet crimes (e.g., social engineering scams or credit card fraud occurring on the Internet). These findings support the notion that the repeal of net neutrality has a deterrent effect on the occurrence of malicious code and content transmitted through data packets, which highlights the role of ISPs as gatekeepers in preventing cybercrime.

This study makes important contributions to the information systems (IS) literature by exploring the intersection between net neutrality and cybersecurity, which has received much attention from IS scholars. Although net neutrality's economic and consumer welfare implications have been widely discussed (Cheng et al. 2011; Guo et al. 2017), empirical investigation of its societal impacts, such as cybercrime and cybersecurity, has been elusive to date. The grand vision of an ICT-Enabled Bright Society (Bright ICT), adopted by the Association for Information Systems (AIS), aims to prevent undesirable activities in cyberspace (Lee 2015). While recent studies have focused on the principle of "origin responsibility" to reduce the negligence of disseminating malicious or wasteful content from origin servers (Ju et al. 2021; Lee 2016; Shin et al. 2018), we present the first empirical evidence of the relationship between net neutrality and cybercrime occurrence, supporting the principle of "deliverer responsibility" for ISPs as content deliverers and information intermediaries (Lee et al. 2018). Moreover, our study provides novel insights into the role of net neutrality and open Internet toward the preventive cybersecurity paradigm: For the paradigm shift in cybersecurity from protection-oriented such as network, operational, and information security enhancement and end-user education to prevention-oriented, net neutrality and the open Internet may need to be carefully considered, given the possible caveat of net neutrality in terms of cybercrime occurrence.

The rest of the paper is organized as follows: In Section 2, we review the background and prior work on net neutrality. In Section 3, we posit the theoretical framework for an empirical analysis of the impacts of net neutrality on cybercrime. We discuss the data and methods in Section 4. Sections 5 and 6 provide the results of the empirical analyses and robustness checks to validate our arguments. In Section 7, we offer a discussion and conclusion of our findings, which discuss the limitations of this work and suggest avenues for future work.

Related Literature

Net neutrality is defined as the "principle of treating all types of Internet traffic equally" (Wu 2003). In net neutrality, CPs can provide content and send data without any prioritization by ISPs, and users are not discriminated against in accessing information and online content on the Internet (Economides and Tåg 2012). Net neutrality is often compared to paid prioritization, which means that an ISP can prioritize traffic from affiliated companies and services by letting those packets jump the queue at the ISP's routers or by creating a separate queue dedicated to their traffic. With the rapid expansion of digital businesses and streaming services, many ISPs have argued for the necessity of paid prioritization, giving favorable treatment to some traffic as it crosses a network, beyond the principle of net neutrality, to manage and control explosive Internet traffic effectively. This has led to intense debates on the role of net neutrality. A case in point is a dispute between the FCC and Comcast, a major ISP in the US. In 2008, the FCC maintained that Comcast violated net neutrality by slowing user access to a file-sharing site and ordered the company

to halt its measure. Comcast appealed this sanction, and the US Court of Appeals ruled in favor of Comcast in 2010 (Rowe et al. 2009). As net neutrality has become entangled in disputes with stakeholders, its implications for economic and social welfare have received considerable attention from policymakers, practitioners, and researchers.

In the extant literature on net neutrality, most studies have focused on its impact on stakeholders, including ISPs, CPs, and Internet users (Cheng et al. 2011; Choi and Kim 2010; Economides and Hermalin 2012; Economides and Tåg 2012; Guo et al. 2013; Kourandi et al. 2015). Prior studies identify specific scenarios and conditions in the presence (or lack) of net neutrality for various business outcomes, such as broadband investment (Briglauer et al. 2021; Choi and Kim 2010; Krämer and Wiewiorra 2012), content innovation (Choi et al. 2018; Guo et al. 2012), and prioritization scheme (Baake and Sudaric 2019; Economides and Hermalin 2012). Cheng et al. (2011) suggest that the repeal of net neutrality leads ISPs to reap benefits from receiving preferential access fees from CPs but reduces the incentive to expand their infrastructure capacity. Easley et al. (2018) propose a techno-economic framework to extend net neutrality into data neutrality (see Easley et al. 2018 for a literature review on research on net neutrality involving ISPs and CPs). As these studies have employed an analytical model or discussed it conceptually, however, little empirical evidence has been offered on the impact of (the repeal of) net neutrality so far.

Few studies have discussed the societal impact of net neutrality. As website performance matters to online retailers (Gallino et al. 2018), ISP's paid prioritization strategies may disproportionally benefit large companies and affluent households, leaving others behind on the Internet (Keith 2017). Net neutrality has often been discussed in connection with social justice, such as data equality (Fisher and Streinz 2021) and racial equality on the Internet (McMurria 2016). In contrast, Glass and Tardiff (2019) argue that "the untold societal damage that both sides claim has relatively little to no factual support" (p. 199). Moreover, despite the considerable social costs of cybercrime, the impact of (the repeal of) net neutrality on cybercrime and cybersecurity has only been discussed conceptually (e.g., Hartmann and Giles 2018), and empirical investigation has been elusive. Therefore, this study aims to illuminate how (the repeal of) net neutrality influences cybercrime that could be mediated via an electronic network, considering the role of ISPs in intervening in online content and data transmission.

Theoretical Framework

Role of ISP in Cybercrime and Cybersecurity

ISPs are uniquely positioned as online content deliverers and gatekeepers on the frontline of cybercrime (Amy and Arwa 2020). According to a 2010 survey, approximately 65% of users attributed the spread and delivery of harmful and malicious content related to cybercrime to ISPs (Dancho 2011). Among various types of cybercrime, closely related to ISPs is malicious code and content (e.g., malware and ransomware) delivered through electronic mediums (e.g., spam email), which often precede subsequent cyberattacks or data breaches. Unnecessary transmission of malicious content could incur huge costs to ISPs, CPs, and users exposed to infected content (Caliendo et al. 2012; Ju et al. 2021; Muncaster 2015).

Previous studies have also emphasized that ISPs, as gatekeepers, are well suited to preventing certain types of cybercrime and malicious content dissemination (Kerr and Gilbert 2004; Lee et al. 2018; Rowe et al. 2009). An ISP's intervention, such as inspecting and blocking data packets for illegal or harmful purposes, can play an important role in achieving high-quality information security (Bauer and Obar 2014). Ju et al. (2021) present evidence that an amendment to the anti-spam policy in South Korea in 2014, which includes a clause about the increased responsibility and authority of ISPs in spam content transmission, reduced the volume of spam originating from Korea by 16.1%. Moreover, Rowe et al. (2009) identify legal liability as one of the key barriers to pursuing ISP-provided security, in that an explicit statement about an ISP's security measure could make the ISP fully or partially liable for a customer's security breach. Lee et al. (2018) highlight that "ISPs do not filter these spam emails because they prefer to maintain network neutrality and do not want to take responsibility for harmful delivery" (p. 72), advocating the principle of deliverer responsibility. Hence, the repeal of net neutrality can make the responsibility and liability of ISPs in cybercrime prevention more explicit among the public, which could give ISPs more incentive toward security investment.

Provided that an ISP's capability to monitor and control Internet traffic and data packets flowing via their networks allows them to filter out suspicious traffic and block malicious content transmission, we expect that the repeal of net neutrality can reduce the number of cybercrimes by preventing them from occurring or being transmitted from their origins. In particular, given that ISPs can observe Internet traffic flowing into and out of their networks if net neutrality is repealed, it arguably has a more salient effect on deterring specific types of cybercrimes mediated by data packets.

Net Neutrality and Potential Offenders' Behavior

Beyond the direct role of ISPs in controlling malicious content transmission, the repeal of net neutrality can indirectly impact the criminal activities of potential offenders in cyberspace. As cybercrime is mainly motivated by economic incentives from monetary values of extorting personal information and attacking computer systems (Hui et al. 2017), the economic theory of crime provides an appropriate theoretical lens to understand potential offenders' behavior (Kshetri 2006; Park et al. 2019). In this theory, criminals are regarded as rational individuals, just like anyone else. This theory posits that potential offenders commit a crime when considering that its benefits outweigh its costs (Becker 1968). Given that cybercrime is often systematically organized rather than the result of individual activities, criminal activities that maximize the interests of both enforcers and criminals are likely to be based on reasonable choices. Before they commit criminal acts in cyberspace, potential offenders would contemplate benefits (e.g., monetary values) and costs of crimes (e.g., opportunity costs of apprehension), as well as success rates of criminal acts and probabilities of apprehension, reshaped by external factors such as policy change.

Given that the anonymous nature of cyberspace activities makes cybercrime investigation extremely difficult (Hui et al. 2017), we conjecture that an increased probability of identification and arrest and lowered success rates of cybercrime due to the repeal of net neutrality will prevent cybercriminals from committing crimes. Criminals recognize and consider the change in circumstances in which they try to commit a crime, for example, owing to crime deterrence policies (Bronars and Lott 1998; Lott and Mustard 1997) and the use of police technologies, such as body-worn cameras (Zamoff et al. 2022) and criminals' DNA profile databases (Doleac 2017). Formal and informal online social control and sanctions are negatively associated with online misconduct (e.g., digital piracy) and system-trespassing offenses (e.g., hacking) (Berenblum et al. 2019; Bossler 2021). Chan et al. (2019a) present empirical evidence that successful policing of darknet participants, which could increase the probability of apprehension on the platform, reduces the number of active vendors and subsequent transactions at the investigated site. Hui et al. (2017) suggest that the enforcement of the Convention on Cybercrime (COC)—the first international legislation against cybercriminal behavior—can reduce distributed denial of service (DDoS) attacks by arguing that "the COC will help deter DDoS attack if potential criminals are rational and aware of the heightened punishment and guardianship in the enforcing countries" (p. 502). Similarly, the repeal of net neutrality can signal an escalated cost of crime due to the probability of arrest to potential offenders in cyberspace. Given that cybercriminals have sophisticated technology, abundant experience, and expertise (Kshetri 2006), the repeal of net neutrality can lead to crime deterrence by raising awareness of the cost of crime (i.e., the lost opportunity for offenders to demonstrate their abilities when arrested). Thus, we expect that the repeal of net neutrality can reduce the motivation of potential offenders to commit cybercrime, as long as they perceive that their online activities can be traced in cyberspace.

Methodology

Data

Considering state-specific legal responses to the repeal of net neutrality, we construct a panel dataset covering 51 states (including the District of Columbia) in the US from 2016 to 2020. We restrict the time window to years when all data sources are available by the current set of variables. Tables 1 and 2 present the descriptions, sources, and summary statistics of the variables used in our analysis.

Table 1. Data Descriptions and Sources

Variable	Description	Data Source
Repeal of net neutrality	1 if the net neutrality has been repealed in the state and 0 otherwise	NCSL

Perpetrator count	# of individuals who perpetrating the scam as reported by the victim (logarithm)	IC3
Victim count	# of individuals who filing as complaint (logarithm)	
Broadband availability	% of fixed residential broadband providers (fixed 25/3 Mbps)	FCC
Download average speed	By averaging state average download speed across all providers in the tract (kbps) (logarithm)	ICPSR
Upload average speed	By averaging state average upload speed across all providers in the tract (kbps) (logarithm)	
Police officer	# of sworn law enforcement officers (logarithm)	FBI UCR
Information industry payroll	% of annual payroll of employees in information industry to the total industry (NACIS 51)	US Census / Bureau of Labor Statistics
Finance and insurance industry payroll	% of annual payroll of employees in finance and insurance industry to the total industry (NACIS 52)	
Professional, scientific, and technical services industry payroll	% of annual payroll of employees in professional, scientific, and technical services industry to the total industry (NACIS 54)	
Population	# of total population (logarithm)	
Median income	Median household income (logarithm)	
Unemployment rate	% of unemployed workers	
Educational attainment	% of adults 25 years old and over with a bachelor diploma or a higher qualification	
Poverty rate	% of below poverty level	

Table 2. Summary Statistics (N = 255)

Variables	Mean	Std. Dev	Min	Max
Dependent Variables				
ln(Perpetrator count_malicious code and content)	4.368	1.184	0.693	7.242
ln(Perpetrator count_malicious attack)	1.462	1.048	0	4.430
ln(Perpetrator count_malicious access)	5.088	1.202	2.639	8.213
ln(Victim count_malicious code and content)	6.154	1.121	3.688	8.825
ln(Victim count_malicious attack)	2.658	1.103	0	5.459
ln(Victim count_malicious access)	6.630	1.124	4.248	9.461
Independent Variables				
Repeal of net neutrality	0.105	0.308	0	1
Control Variables				
Broadband availability	0.797	0.264	0.005	0.993
ln(Download average speed)	4.802	0.656	2.678	6.362
ln(Upload average speed)	4.152	0.815	1.905	6.134
ln(Police officer)	8.960	1.061	6.896	11.285
Information industry payroll	0.038	0.023	0.015	0.173
Finance and insurance industry payroll	0.085	0.034	0.033	0.212
Professional, scientific, and technical services industry payroll	0.100	0.049	0.042	0.331
ln(Population)	15.168	1.034	13.269	17.490
ln(Median income)	11.030	0.174	10.640	11.429
Unemployment rate	0.047	0.017	0.022	0.128
Educational attainment	0.321	0.064	0.202	0.615
Poverty rate	0.126	0.028	0.070	0.210

Our main treatment of interest is the repeal of net neutrality, enacted in 2018. Thus, our treatment group involves states that did not take any legal action and respected the FCC's decision to repeal net neutrality, so they have been affected by it since 2018. In contrast, the control group includes states that implemented or initiated their own rules to support net neutrality, and net neutrality has been in place even after 2018. To identify state-level responses to federal action toward the repeal of net neutrality, we obtain information about legal responses in each state from the National Conference of State Legislature's (NCSL) net neutrality legislation.[1] Thirty-four states and the District of Columbia proposed or passed bills and resolutions to maintain net neutrality in 2018–2019. For instance, California passed the California Internet Consumer Protection and Net Neutrality Act of 2018,[2] which prohibits ISPs from engaging in actions concerning Internet traffic. Table 3 summarizes state-specific legal responses to the repeal of net neutrality.

Table 3. State-Specific Legal Responses to the Repeal of Net Neutrality in the US

State	Status	State	Status	State	Status
(1)	(2)	(3)	(4)	(5)	(6)
Alabama	-	Kentucky	Bill proposed in 2018	North Dakota	-
Alaska	Bill proposed in 2018	Louisiana	-	Ohio	Bill proposed in 2018
Arizona	-	Maine	Bill passed in 2019	Oklahoma	Bill proposed in 2018
Arkansas	-	Maryland	Bill proposed in 2018	Oregon	Bill passed in 2018
California	Bill passed in 2018	Massachusetts	Bill proposed in 2018	Pennsylvania	Bill proposed in 2018
Colorado	Bill proposed in 2018 / Bill passed in 2019	Michigan	Bill proposed in 2018	Rhode Island	Executive order in 2018
Connecticut	Bill proposed in 2018	Minnesota	Bill proposed in 2018	South Carolina	Bill proposed in 2018
Delaware	Bill proposed in 2018	Mississippi	-	South Dakota	Bill proposed in 2018
District of Columbia	Bill proposed in 2018	Missouri	Bill proposed in 2018	Tennessee	Bill proposed in 2018
Florida	-	Montana	Executive order in 2018	Texas	Bill proposed in 2019
Georgia	Bill proposed in 2018	Nebraska	Bill proposed in 2018	Utah	Bill proposed in 2019
Hawaii	Executive order in 2018	Nevada	Bill proposed in 2019	Vermont	Bill passed in 2018
Idaho	Bill proposed in 2018	New Hampshire	Bill proposed in 2019	Virginia	Bill proposed in 2018
Illinois	Bill proposed in 2018	New Jersey	Bill passed in 2018	Washington	Bill passed in 2018
Indiana	-	New Mexico	Bill proposed in 2018	West Virginia	Bill proposed in 2018
Iowa	Bill proposed in 2018	New York	Executive order in 2018	Wisconsin	Bill proposed in 2018
Kansas	Bill proposed in 2018	North Carolina	Bill proposed in 2018	Wyoming	-

Source: National Conference of State Legislature

For dependent variables, we obtain data on the yearly number of cybercrime subjects (perpetrators) and victims at the state level from the IC3 annual reports.[3] As IC3 compiles a broad range of crimes that

[1] Source: https://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-legislation-in-states.aspx (2018 legislation); https://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-2019-legislation.aspx (2019 legislation); and https://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-2020-legislation.aspx (2020 legislation).

[2] See https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB822

[3] IC3 provides the subject (perpetrator) count identified as individuals perpetrating the scam as reported by the victim for each state and the victim count identified as individuals filing a complaint. The IC3 annual reports that include perpetrators and victims for

occur on the Internet, we separate cybercrime, which involves computer systems, from general Internet crimes. We then classify cybercrime into (i) malicious code and content that are transmitted through data packets to compromise computer systems and devices (termed "malicious code and content" hereafter), (ii) attacks on target servers and networks based on compromised systems (termed "malicious attack"), (iii) breaches of data due to compromised systems or some human factors such as device loss or accidental or malicious insiders (termed "malicious access"). Malicious code and content include business email compromises, phishing, malware, and ransomware.[4] Malicious attacks include denial-of-service, hacktivist, and terrorist attacks. Malicious access includes data breaches (corporate and personal) and identity theft. To investigate the relationship between the repeal of net neutrality and criminal activities, we consider both subject and victim counts as dependent variables.

To control for Internet penetration rates over the years, we include the number of fixed residential broadband services of at least 25Mbps download and 3Mbps upload around the states (Park et al. 2019) and average download/upload speeds across all providers in the state, which are obtained from the FCC and the Inter-university Consortium for Political and Social Research (ICPSR), respectively.[5] We control for the number of police officers provided by the data from the Uniform Crime Reporting (UCR) program compiled by the Federal Bureau of Investigation (FBI) to reflect the state's overall security level (Chan et al. 2016; Chan et al. 2019b; Park et al. 2021). Given that the information-intensive industries are likely more involved in cybercrime than other industries, we control for the percentage of annual payroll for information, finance and insurance, and professional, scientific, and technical industries to the total industry (NACIS 51, 52, and 54). To this end, we utilize state-level payroll information in each industry to proxy its size, as reported by the County Business Pattern of the Census Bureau. We also consider socioeconomic and demographic factors that could influence cybercriminal activities, including unemployment rate, population, median income, educational attainment, and poverty rate (Hui et al. 2017; Ju et al. 2021; Park et al. 2019).

Empirical Model

We exploit a natural experiment in which the repeal of net neutrality took effect in 2018 across the United States, while some states denied federal legislation by introducing state-level legislation to support net neutrality. To identify the impact of the repeal of net neutrality, we estimate the following DID model for state i in year t:

$$y_{it} = \alpha_i + \beta(Repeal\ of\ Net\ Neutrality)_{it} + Z_{it}\gamma + \theta_i + \lambda_t + \varepsilon_{it}, \quad (1)$$

where y_{it} is the logarithm of the number of cybercrime occurrences and $Repeal\ of\ Net\ Neutrality_{it}$ is a dichotomous variable that indicates whether the repeal of net neutrality exists in a given year.[6] To account for confounding factors, we include the set of control variables listed in Table 1 (Z_{it}). Additionally, state fixed effects (θ_i) and year fixed effects (λ_t) are considered to control state-specific heterogeneity and nationwide trends in cybercriminal activities and Internet policies. Note that we log-transform all continuous variables, except the percentage measures, to correct for skewness.

The key assumption for the DID model is whether it represents a parallel trend in the outcome of interest across the treatment and control groups during the pretreatment period (Angrist and Pischke 2008). To validate the parallel trend assumption, we employ the relative time model, as has been widely used in prior studies (Burtch et al. 2018; Greenwood and Agarwal 2016). Specifically, our DID model is extended as follows:

---

the current crime categories are available from 2016 (https://www.ic3.gov/Home/AnnualReports). This dataset has been used to study the perpetrators of cybercrime (Park et al. 2019).

[4] Spoofing was not considered as this category was not included in 2016 data.

[5] See https://broadbandmap.fcc.gov and https://www.openicpsr.org/openicpsr/project/128841/version/V2/view.

[6] While states proposed and passed bills or executive orders to support net neutrality at different times (see Table 3), we consider all states that took any legal action in 2018–2019 as the control group for a clearer research design. This is because states could signal the support of net neutrality to ISPs and potential offenders even before formal legislation. However, we also consider staggering legislation across states in defining the treatment and control groups as a robustness check.

$$y_{it} = \alpha + \sum Rel\_Time\_Repeal\ of\ Neutrality_{it} + Z_{it}\gamma + \theta_i + \lambda_t + \varepsilon_{it}, \quad (2)$$

where $Repeal\ of\ Net\ Neutrality_{it}$ is replaced with a vector of relative time dummies $\sum Rel\_Time\_Repeal\ of\ Neutrality_{it}$, which indicates the relative temporal distance from the treatment timing. Given that the rep eal of net neutrality took effect in 2018, we consider dummy variables that indicate each year for the treate d states. All control variables and the state- and year fixed effects are applied in the same way as in the ma in analysis.

Results

Impact of the Repeal of Net Neutrality on Cybercrime

Table 4 presents the estimation results of the DID model, and Columns 1–3 (Columns 4–6) show the results for the number of perpetrators (victims). In Column 1, we find that the repeal of net neutrality is negatively associated with the number of perpetrators for the occurrence of malicious code and content. The coefficient translates into a 34.0% ($= e^{0.293} - 1$) reduction in the number of malicious code and content transmitted via data packets following the repeal of net neutrality, which is economically significant. As we have argued, the repeal of net neutrality serves as crime deterrence by enabling ISPs to observe and track data packets. However, the repeal of net neutrality is found to have insignificant effects on the number of perpetrators of malicious attacks and accesses, as shown in Columns 2 and 3, which means that it is not related to cybercrime that may subsequently occur in compromised systems. In contrast, Columns 4 to 6 demonstrate that the repeal of net neutrality has no significant relationship to the victim count for any type of cybercrime. These findings imply that the repeal of net neutrality plays a role in preventing cybercrime, not protecting users from cybercrime.

Table 4. Estimation Results for the Repeal of Net Neutrality and Cybercrime

Dependent Variable:	Perpetrator Count			Victim Count		
	Malicious code and content	Malicious attack	Malicious access	Malicious code and content	Malicious attack	Malicious access
	(1)	(2)	(3)	(4)	(5)	(6)
Repeal of Net Neutrality	-0.293***	0.113	0.108	-0.022	0.151	0.084
	(0.094)	(0.195)	(0.076)	(0.066)	(0.159)	(0.061)
Broadband availability	-0.118	-0.071	0.048	-0.266*	0.063	-0.035
	(0.194)	(0.343)	(0.134)	(0.147)	(0.299)	(0.127)
ln(Download average speed)	0.112	-0.024	0.010	0.052	-0.121**	0.018
	(0.078)	(0.087)	(0.038)	(0.037)	(0.060)	(0.026)
ln(Upload average speed)	-0.089*	-0.034	-0.054	-0.028	0.063	-0.043
	(0.049)	(0.073)	(0.062)	(0.039)	(0.081)	(0.035)
ln(Police officer)	-0.122	-0.021	-0.328	0.070	-0.205	0.045
	(0.110)	(0.370)	(0.336)	(0.069)	(0.153)	(0.075)
Information industry payroll	-8.726	-15.180	2.321	0.118	-7.828	-2.160
	(5.674)	(14.004)	(4.867)	(3.447)	(7.229)	(4.646)
Finance and insurance industry payroll	7.769	3.114	16.227***	1.727	-9.262	-3.092
	(5.771)	(14.994)	(5.031)	(5.786)	(8.812)	(6.975)
Professional, scientific, and technical services industry payroll	-1.676	-4.617	-11.609	-0.651	-15.498	-7.549
	(11.285)	(11.637)	(8.287)	(4.555)	(11.819)	(6.563)
ln(Population)	-2.365	-0.259	-2.675	2.477	0.304	3.266
	(2.006)	(4.439)	(2.504)	(1.511)	(2.156)	(3.200)
ln(Median income)	1.776	-3.561	0.498	-0.843	1.973	0.749
	(2.161)	(4.428)	(1.346)	(1.261)	(3.235)	(1.434)
Unemployment rate	-5.429**	4.071	-1.015	-2.719	1.396	6.163
	(2.265)	(6.207)	(3.867)	(3.353)	(3.841)	(6.796)

Educational attainment	-2.560	11.616	-2.025	-0.645	-2.112	-0.275
	(7.036)	(8.779)	(3.546)	(2.804)	(8.452)	(3.306)
Poverty rate	6.304	-0.700	7.508	1.563	10.112	4.835
	(6.459)	(14.641)	(5.361)	(5.011)	(11.399)	(3.884)
State fixed effects	YES	YES	YES	YES	YES	YES
Year fixed effects	YES	YES	YES	YES	YES	YES
R-squared	0.974	0.848	0.976	0.980	0.917	0.983
Observations	255	255	255	255	255	255

Notes: Robust standard errors clustered by state are shown in parentheses; ***p<0.01, **p<0.05, *p<0.1.

Table 5 shows the results of the relative time model, in which the year 2017 serves as a baseline. The results suggest no significant difference between the treated and control groups during the pre-treatment period for any type of cybercrime, indicating that the treatment and control groups are comparable when net neutrality was in place nationwide. In keeping with our main result, the posttreatment coefficients become significantly negative only for the occurrence of malicious code and content. This suggests that the impact of the repeal of net neutrality on cybercrime based on malicious code and content transmission via data packets manifests immediately and lasts longer albeit a smaller impact size in the later years.

Table 5. Estimation Results of the Relative Time Model

Dependent Variable:	Perpetrator Count		
	Malicious code and content	Malicious attack	Malicious access
	(1)	(2)	(3)
$Repeal\ of\ Net\ Neutrality_{t=-2}$	-0.115	0.135	-0.016
	(0.103)	(0.345)	(0.074)
$Repeal\ of\ Net\ Neutrality_{t=-1}$	Omitted as a baseline		
$Repeal\ of\ Net\ Neutrality_{t=0}$	-0.465**	0.133	0.038
	(0.174)	(0.247)	(0.099)
$Repeal\ of\ Net\ Neutrality_{t=1}$	-0.246**	0.255	0.156
	(0.112)	(0.400)	(0.123)
$Repeal\ of\ Net\ Neutrality_{t=2}$	-0.253**	-0.238	0.067
	(0.121)	(0.351)	(0.103)
Control variables	YES	YES	YES
State fixed effects	YES	YES	YES
Year fixed effects	YES	YES	YES
R-squared	0.975	0.852	0.976
Observations	255	255	255

Notes: Robust standard errors clustered by state are shown in parentheses; All control variables reported in Table 4 are included; ***p<0.01, **p<0.05, *p<0.1.

Robustness Checks

We conduct robustness checks to substantiate our findings. First, one might be concerned that states that took legal actions to maintain net neutrality in 2019 (i.e., Maine, Nevada, New Hampshire, Texas, and Utah) could be differentiated from other states in the control group that responded immediately in 2018. To test whether our findings are sensitive to composition of the treatment and control groups in the DID model, we estimate the DID model with an alternative treatment indicator by considering that the five states with late responses were temporarily affected the repeal of net neutrality in 2018. Additionally, we replicate the analysis after excluding states with late responses. Table 6 demonstrates that different timings of state-specific legal responses are not likely alter our main findings.

Table 6. Accounting for Different Timing of State-Specific Legal Responses

Dependent Variable:	Alternative Definition of the Treatment			Exclusion of States with Late Responses		
	Perpetrator Count					
	Malicious code and content	Malicious attack	Malicious access	Malicious code and content	Malicious attack	Malicious access

	(1)	(2)	(3)	(4)	(5)	(6)
Repeal of Net Neutrality	-0.237***	0.068	0.053	-0.282***	0.137	0.106
	(0.079)	(0.162)	(0.078)	(0.101)	(0.194)	(0.075)
Control variables	YES	YES	YES	YES	YES	YES
State fixed effects	YES	YES	YES	YES	YES	YES
Year fixed effects	YES	YES	YES	YES	YES	YES
R-squared	0.974	0.848	0.976	0.976	0.852	0.976
Observations	255	255	255	230	230	230

Notes: Robust standard errors clustered by state are shown in parentheses; All control variables reported in Table 4 are included; ***p<0.01, **p<0.05, *p<0.1.

Second, we conduct falsification tests using different crimes that are unlikely to be affected by the repeal of net neutrality as the alternative dependent variables. In doing so, we obtain the number of property and violent crime incidents from the FBI's UCR program. We also consider general Internet crimes that occur in cyberspace (e.g., social engineering scams or credit card frauds on the Internet). We define general Internet crime as the sum of all Internet crimes available from the IC3 dataset less than cybercrime involving the computer systems used in the main analysis. Table 7 shows that the repeal of net neutrality is not significantly associated with different types of crimes, which lends credence to our main findings on the significant relationship between the repeal of net neutrality and the occurrence of malicious code and content.

Table 7. Falsification Tests for Other Crimes

Dependent Variable:	Number of Incidents		Perpetrator Count	Victim Count
	Property crime	Violent crime	General Internet crime, other than cybercrime	
	(1)	(2)	(3)	(4)
Repeal of Net Neutrality	-0.021	-0.015	-0.016	-0.031
	(0.022)	(0.022)	(0.075)	(0.061)
Control variables	YES	YES	YES	YES
State fixed effects	YES	YES	YES	YES
Year fixed effects	YES	YES	YES	YES
R-squared	0.998	0.998	0.982	0.990
Observations	255	255	255	255

Notes: Robust standard errors clustered by state are shown in parentheses; All control variables reported in Table 4 are included; ***p<0.01, **p<0.05, *p<0.1.

Discussion and Conclusion

The Internet has been interwoven into daily lives, like electricity, driving businesses, and connecting people online more easily than ever. The fast-paced evolution of Internet technology presents opportunities (e.g., new business models such as digital platforms and metaverse) and challenges (e.g., invasion of privacy and exposure to cybercrime). This makes policymakers and researchers pay more attention to new technologies and policies toward the faster, safer, and more inclusive Internet. This study presents a fresh perspective on the future of the Internet by examining the role of net neutrality for the open Internet in cybercrime.

We present what we believe to be the first empirical evidence of the positive (negative) relationship between (the repeal of) net neutrality and cybercrime occurrence. Specifically, our findings suggest that the repeal of net neutrality in the US, which allows ISPs to access and control data packets to a certain extent, reduces the occurrence of malicious code and content (i.e., malicious messages) transmitted via the network, such as malware and ransomware, but does not influence cybercrime victimization. The results highlight the critical role of ISPs as online content deliverers and information intermediaries in cybercrime prevention, rather than cybercrime protection on the user side. Although equal access and transmission of online content, regardless of its source and content, has been considered sacred on the Internet, our findings imply that surveillance and control of online content and data packets, to a certain extent, but in a regulated manner, may be inevitable to transform cybersecurity paradigms from protection-oriented to prevention-oriented. This study can inform ongoing debates on net neutrality and the future of the Internet by shedding new light on the possible caveat of net neutrality and open Internet in terms of cybercrime and cybersecurity.

This study contributes to the IS literature on net neutrality (Easley et al. 2018; Guo et al. 2017; Kourandi et al. 2015; Krämer and Wiewiorra 2012). Prior studies have utilized an analytical modeling approach to study how net neutrality's presence (or lack) influences stakeholders (i.e., ISP, CP, and consumers), such as quality of service tiering (Krämer and Wiewiorra 2012), broadband investment (Cheng et al. 2011), Internet fragmentation (Kourandi et al. 2015), network management (Cho et al. 2016), and competition among ISPs and CPs (Guo et al. 2017). To the best of our knowledge, this study is the first empirical research to investigate the societal impact of net neutrality, particularly cybercrime and cybersecurity. This study advances the body of knowledge about the role of net neutrality by exploring its relationship to cybercrime by leveraging a natural experiment involving the repeal of net neutrality in the US, which can be adopted in future research to study socio-economic impacts of the repeal of net neutrality. We also adopt an interdisciplinary approach that is commonly used to examine the societal impacts of IT and IS (Chan et al. 2016; Cheng et al. 2020; Park et al. 2021). Guided by the economic theory of crime, we substantiate the mechanism by which the repeal of net neutrality contributes to a reduction in the occurrence of malicious code and content transmitted through data packets on the Internet by deterring criminal activities of potential cybercriminals, rather than protecting users from cyberattacks and data breaches.

Furthermore, this study extends the strand of research that aims to prevent harmful and malicious conduct on the Internet pursued by AIS's Bright ICT initiative (Lee 2015; Lee et al. 2020; Shin et al. 2018). As a core project of the Bright ICT initiative, the Bright Internet builds upon two principles in terms of the locus of responsibility for cybercrime: origin responsibility and deliverer responsibility. Although recent studies have been conducted with an abundance of evidence on the principle of origin responsibility to reduce the negligence of disseminating malicious or wasteful content from origin servers (Ju et al. 2021; Lee 2016; Shin et al. 2018), we cast new light on the relationship between net neutrality and cybercrime occurrence. This highlights the significant role of ISPs as content deliverers and supports the principle of deliverer responsibility (Lee et al. 2018). Thus, our study implies that for the paradigm shift in cybersecurity from protection-oriented to prevention-oriented, net neutrality and the open Internet need to be taken seriously, as it has significant implications on cybercrime and cybersecurity.

This study has some limitations. First, while we analyze state-level responses to the repeal of net neutrality, the effect of net neutrality may vary depending on the local socio-political environments and industry structures of ISPs and CPs. Additionally, perceptions and responses to net neutrality and openness of the Internet may exhibit cultural differences across countries. Thus, future research could extend our findings to other countries or investigate it at a more granular level, such as city level, if data is available, to offer deeper insights into the heterogeneous roles of net neutrality. Second, this study could not account for cross-border cybercrime (Kim et al. 2012) as our dataset includes cybercriminals and victims who are known to reside within the US. Given that net neutrality may reshape cyber warfare (Hartmann and Giles 2018), future researchers could examine how the repeal of net neutrality influences cybercrime, cyberattacks, and cyberterrorism originating from foreign countries. Third, we cannot observe situations and circumstances in which potential cybercriminals are situated. As our theoretical arguments imply that changed criminal environments can have a deterrent effect on potential cybercriminals, further research might benefit from direct access to perpetrators' profiles or interviews to understand their motivations in the face of policy change in depth.

Despite these limitations, this study can attract the attention of legal authorities and policymakers and provide meaningful practical implications. Debate and public discourse on the role, authority, and responsibility of ISPs due to repeal of net neutrality focus on direct economic benefits among stakeholders, but we suggest that the repeal of net neutrality can also have a societal impact. Given that the repeal of net neutrality allows ISPs to act as gatekeepers to control data packets, our findings suggest that repeal of net neutrality can be a valuable means of deterring cybercrime. In addition, our findings can provide new evidence of the societal impact caused by the repeal of net neutrality for legal authorities and policymakers, while further extending the depth of Internet policy effectiveness and underpinning well-designed regulations and policy measures. We hope that our theoretical approaches and empirical findings will also be applied to various societal problems in the future, becoming an avenue for future research.

References

Akdeniz, Y. 2002. "Anonymity, Democracy, and Cyberspace," *Social Research: An International Quarterly* (69:1), pp. 223-237.

Amy, J., and Arwa, A. 2020. "4 Things ISPs Can Do to Reduce the Impact of Cybercrime," from https://www.weforum.org/agenda/2020/01/heres-what-isps-should-be-doing-to-tackle-cybercrime/

Angrist, J. D., and Pischke, J.-S. 2008. *Mostly Harmless Econometrics: An Empiricist's Companion*, Princeton, NJ: Princeton University Press.

Baake, P., and Sudaric, S. 2019. "Net Neutrality and CDN Intermediation," *Information Economics and Policy* (46), pp. 55-67.

Bauer, J. M., and Obar, J. A. 2014. "Reconciling Political and Economic Goals in the Net Neutrality Debate," *The Information Society* (30:1), pp. 1-19.

Becker, G. S. 1968. "Crime and Punishment: An Economic Approach," *Journal of Political Economy* (76:2), pp. 169-217.

Berenblum, T., Weulen Kranenbarg, M., and Maimon, D. 2019. "Out of Control Online? A Combined Examination of Peer-Offending and Perceived Formal and Informal Social Control in Relation to System-Trespassing," *Journal of Crime and Justice* (42:5), pp. 616-631.

Bossler, A. M. 2021. "Perceived Formal and Informal Sanctions in Deterring Cybercrime in a College Sample," *Journal of Contemporary Criminal Justice* (37:3), pp. 452-470.

Briglauer, W., Cambini, C., Gugler, K., and Stocker, V. 2021. "Net Neutrality and High Speed Broadband Networks: Evidence from OECD Countries," in *Proceedings of the 23rd Biennial Conference of the International Telecommunications Society (ITS)*.

Bronars, S. G., and Lott, J. R. 1998. "Criminal Deterrence, Geographic Spillovers, and the Right to Carry Concealed Handguns," *The American Economic Review* (88:2), pp. 475-479.

Burtch, G., Carnahan, S., and Greenwood, B. N. 2018. "Can You Gig It? An Empirical Examination of the Gig Economy and Entrepreneurial Activity," *Management Science* (64:12), pp. 5497-5520.

Caliendo, M., Clement, M., Papies, D., and Scheel-Kopeinig, S. 2012. "Research Note—the Cost Impact of Spam Filters: Measuring the Effect of Information System Technologies in Organizations," *Information Systems Research* (23:3), pp. 1068-1080.

Cerf, V. G. 2022. "Preserving the Internet," *Communications of the ACM* (65:4), p. 5.

Chan, J., Ghose, A., and Seamans, R. 2016. "The Internet and Racial Hate Crime: Offline Spillovers from Online Access," *MIS Quarterly* (40:2), pp. 381-403.

Chan, J., He, S., Qiao, D., and Whinston, A. B. 2019a. "Shedding Light on the Dark: The Impact of Legal Enforcement on Darknet Transactions," NET Institute Working Paper 19-08, Networks, Electronic Commerce and Telecommunications Institute, New York.

Chan, J., Mojumder, P., and Ghose, A. 2019b. "The Digital Sin City: An Empirical Study of Craigslist's Impact on Prostitution Trends," *Information Systems Research* (30:1), pp. 219-238.

Cheng, H. K., Bandyopadhyay, S., and Guo, H. 2011. "The Debate on Net Neutrality: A Policy Perspective," *Information Systems Research* (22:1), pp. 60-82.

Cheng, Z., Pang, M.-S., and Pavlou, P. A. 2020. "Mitigating Traffic Congestion: The Role of Intelligent Transportation Systems," *Information Systems Research* (31:3), pp. 653-674.

Cho, S., Qiu, L., and Bandyopadhyay, S. 2016. "Should Online Content Providers Be Allowed to Subsidize Content?—An Economic Analysis," *Information Systems Research* (27:3), pp. 580-595.

Choi, J. P., Jeon, D. S., and Kim, B. C. 2018. "Net Neutrality, Network Capacity, and Innovation at the Edges," *The Journal of Industrial Economics* (66:1), pp. 172-204.

Choi, J. P., and Kim, B. C. 2010. "Net Neutrality and Investment Incentives," *The RAND Journal of Economics* (41:3), pp. 446-471.

Chuck, B. 2021. "More Alarming Cybersecurity Stats for 2021 !," from https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/?sh=6a26ca9b4a36/

Dancho, D. 2011. "Dear ISP, It's Time to Quarantine Your Malware-Infected Customers," from https://www.zdnet.com/article/dear-isp-its-time-to-quarantine-your-malware-infected-customers/

Doleac, J. L. 2017. "The Effects of DNA Databases on Crime," *American Economic Journal: Applied Economics* (9:1), pp. 165-201.

Easley, R. F., Guo, H., and Krämer, J. 2018. "Research Commentary—From Net Neutrality to Data Neutrality: A Techno-Economic Framework and Research Agenda," *Information Systems Research* (29:2), pp. 253-272.
Economides, N., and Hermalin, B. E. 2012. "The Economics of Network Neutrality," *The RAND Journal of Economics* (43:4), pp. 602-629.
Economides, N., and Tåg, J. 2012. "Network Neutrality on the Internet: A Two-Sided Market Analysis," *Information Economics and Policy* (24:2), pp. 91-104.
Fisher, A., and Streinz, T. 2021. "Confronting Data Inequality," Institute for International Law and Justice Working Paper.
Forman, C. 2005. "The Corporate Digital Divide: Determinants of Internet Adoption," *Management Science* (51:4), pp. 641-654.
Gallino, S., Karacaoglu, N., and Moreno, A. 2018. "Why Retailers Should Care About Net Neutrality: The Impact of Website Performance on Online Retail," Available at SSRN 3260203.
Genachowski, J. 2010. "Preserving a Free and Open Internet," from https://www.fcc.gov/news-events/blog/2010/12/01/preserving-free-and-open-internet/
Glass, V., and Tardiff, T. 2019. "A New Direction for the Net Neutrality Debate," *Telecommunications Policy* (43:3), pp. 199-212.
Goel, S. 2015. "Anonymity vs. Security: The Right Balance for the Smart Grid," *Communications of the Association for Information Systems* (36), pp. 23-32.
Greenwood, B. N., and Agarwal, R. 2016. "Matching Platforms and HIV Incidence: An Empirical Investigation of Race, Gender, and Socioeconomic Status," *Management Science* (62:8), pp. 2281-2303.
Guo, H., Bandyopadhyay, S., Lim, A., Yang, Y.-C. B., and Cheng, H. K. 2017. "Effects of Competition among Internet Service Providers and Content Providers on the Net Neutrality Debate," *MIS Quarterly* (41:2), pp. 353-370.
Guo, H., Cheng, H. K., and Bandyopadhyay, S. 2012. "Net Neutrality, Broadband Market Coverage, and Innovation at the Edge," *Decision Sciences* (43:1), pp. 141-172.
Guo, H., Cheng, H. K., and Bandyopadhyay, S. 2013. "Broadband Network Management and the Net Neutrality Debate," *Production and Operations Management* (22:5), pp. 1287-1298.
Hadley, T. 2018. "Anonymizer Supports Network Neutrality by Preserving Online Anonymity," from https://www.businesswire.com/news/home/20180123005158/en/Anonymizer-Supports-Network-Neutrality-by-Preserving-Online-Anonymity/
Hartmann, K., and Giles, K. 2018. "Net Neutrality in the Context of Cyber Warfare," in *Proceedings of the 10th International Conference on Cyber Conflict (CyCon): NATO CCD COE Publications*, pp. 139-158.
Hoffman, D. L., Novak, T. P., and Venkatesh, A. 2004. "Has the Internet Become Indispensable?," *Communications of the ACM* (47:7), pp. 37-42.
Hui, K.-L., Kim, S. H., and Wang, Q.-H. 2017. "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks," *MIS Quarterly* (41:2), pp. 497-523.
Hyman, P. 2013. "Cybercrime: It's Serious, But Exactly How Serious?," *Communications of the ACM* (56:3), pp. 18-20.
Jamison, M. A. 2018. "Net Neutrality Policies and Regulation in the United States," *Review of Network Economics* (17:3), pp. 151-173.
Ju, J., Cho, D., Lee, J. K., and Ahn, J. H. 2021. "Can It Clean Up Your Inbox? Evidence from South Korean Anti-Spam Legislation," *Production and Operations Management* (30:8), pp. 2636-2652.
Keith, C. 2017. "Why Net Neutrality Was Repealed and How It Affects You," from https://www.nytimes.com/2017/12/14/technology/net-neutrality-rules.html/
Kerr, I. R., and Gilbert, D. 2004. "The Role of ISPs in the Investigation of Cybercrime," In T. Mendina & J. Britz (Eds.), *Information Ethics in the Electronic Age: Current Issues in Africa and the World*, Jefferson, NC: McFarland, pp. 163-172.
Kim, S. H., Wang, Q.-H., and Ullrich, J. B. 2012. "A Comparative Study of Cyberattacks," *Communications of the ACM* (55:3), pp. 66-73.
Kling, R., Lee, Y.-c., Teich, A., and Frankel, M. S. 1999. "Assessing Anonymous Communication on the Internet: Policy Deliberations," *The Information Society* (15:2), pp. 79-90.
Kourandi, F., Krämer, J., and Valletti, T. 2015. "Net Neutrality, Exclusivity Contracts, and Internet Fragmentation," *Information Systems Research* (26:2), pp. 320-338.

Krämer, J., and Wiewiorra, L. 2012. "Network Neutrality and Congestion Sensitive Content Providers: Implications for Content Variety, Broadband Investment, and Regulation," *Information Systems Research* (23:4), pp. 1303-1321.
Kshetri, N. 2006. "The Simple Economics of Cybercrimes," *IEEE Security & Privacy* (4:1), pp. 33-39.
Lee, J. K. 2015. "Research Framework for AIS Grand Vision of the Bright ICT Initiative," *MIS Quarterly* (39:2), pp. iii-xii.
Lee, J. K. 2016. "Reflections on ICT-Enabled Bright Society Research," *Information Systems Research* (27:1), pp. 1-5.
Lee, J. K., Chang, Y., Kwon, H. Y., and Kim, B. 2020. "Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach," *Information Systems Frontiers* (22:1), pp. 45-57.
Lee, J. K., Cho, D., and Lim, G. G. 2018. "Design and Validation of the Bright Internet," *Journal of the Association for Information Systems* (19:2), pp. 63-85.
Lott, J., John R, and Mustard, D. B. 1997. "Crime, Deterrence, and Right-to-Carry Concealed Handguns," *The Journal of Legal Studies* (26:1), pp. 1-68.
Manyika, J., and Roxburgh, C. 2011. *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity*, McKinsey Global Institute.
McMurria, J. 2016. "From Net Neutrality to Net Equality," *International Journal of Communication* (10), pp. 5931-5948.
Muncaster, P. 2015. "Spam Volumes Drop but Unsolicited Emails Get More Malicious," from https://www.infosecurity-magazine.com/news/spam-volumes-drop-unsolicited/
Nguyen, V., Mohammed, D., Omar, M., and Dean, P. 2020. "Net Neutrality around the Globe: A Survey," in *Proceedings of the 3rd International Conference on Information and Computer Technologies (ICICT)*, pp. 480-488.
Ohm, P. 2010. "When Network Neutrality Met Privacy," *Communications of the ACM* (53:4), pp. 30-32.
Park, J., Cho, D., Lee, J. K., and Lee, B. 2019. "The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status," *ACM Transactions on Management Information Systems* (10:4), pp. 1-23.
Park, J., Pang, M.-S., Kim, J., and Lee, B. 2021. "The Deterrent Effect of Ride-Sharing on Sexual Assault and Investigation of Situational Contingencies," *Information Systems Research* (32:2), pp. 497-516.
Rowe, B., Reeves, D., and Gallaher, M. 2009. *The Role of Internet Service Providers in Cyber Security*, Institute for Homeland Security Solutions, June.
Schwartz, P. M. 1999. "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* (52), pp. 1609-1702.
Shin, Y. Y., Lee, J. K., and Kim, M. 2018. "Preventing State-Led Cyberattacks Using the Bright Internet and Internet Peace Principles," *Journal of the Association for Information Systems* (19:3), pp. 152-181.
Steve, M. 2020. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
UNODC. 2019. "Obstacles to Cybercrime Investigations," from https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html
Walsh, K. 2017. "The FCC Pretends to Support Net Neutrality and Privacy While Moving to Gut Both," from https://www.eff.org/deeplinks/2017/05/why-losing-title-ii-means-losing-net-neutrality-and-privacy
Wu, T. 2003. "Network Neutrality, Broadband Discrimination," *Journal on Telecommunications and High Technology Law* (2), pp. 141-179.
Zamoff, M. E., Greenwood, B. N., and Burtch, G. 2022. "Who Watches the Watchmen: Evidence of the Effect of Body-Worn Cameras on New York City Policing," *The Journal of Law, Economics, and Organization* (38:1), pp. 161-195.
Zhuravskaya, E., Petrova, M., and Enikolopov, R. 2020. "Political Effects of the Internet and Social Media," *Annual Review of Economics* (12), pp. 415-438.