COUNTERING THE MALICIOUS USE OF SOCIAL MEDIA

GOVERNMENT RESPONSES TO MALICIOUS USE OF SOCIAL MEDIA

Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard

ISBN 978-9934-564-31-4

ISBN: 978-9934-564-31-4
Authors: **Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard**
Project manager: Sebastian Bay
Text editor: Anna Reynolds
Design: Kārlis Ulmanis

Riga, November 2018
NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

Samantha Bradshaw is a D.Phil. Candidate at the Oxford Internet Institute and a researcher on the Computational Propaganda Project at Oxford University. Samantha has published several journal articles and public policy papers at the nexus of technology, governance and politics. Samantha holds an MA in Global Governance and a BA (joint-honours) in political science and legal studies from the University of Waterloo.

Lisa-Maria Neudert is a DPhil candidate at the Oxford Internet Institute and a researcher with the Computational Propaganda project. Lisa-Maria holds a MSc in Social Science of the Internet from the University of Oxford, a BA in Communication Science from the Ludwig-Maxmilians-University in Munich and an Honors Degree in International Diplomacy from Georgetown University. She was selected as a Fulbright scholar.

Philip N. Howard is a professor and writer. He has written numerous empirical research articles, and published in a number of disciplines, on the use of digital media for both civic engagement and social control in countries around the world. Howard is a statutory Professor of Internet Studies at the Oxford Internet Institute and a Senior Fellow at Balliol College at the University of Oxford.

INTRODUCTION

The manipulation of public opinion regarding social media during critical moments of political life has emerged as a pressing policy concern. During the 2016 Presidential Election in the United States and the Brexit Referendum in the United Kingdom reports about the malicious use of social media and the exploitation of personal data for political gain rose to global prominence, prompting legal and regulatory intervention by governments around the world. But the use of social media to undermine democracy has long been a concern for NATO and the European security community.

Since 2016, at least 43 countries around the globe have proposed or implemented regulations specifically designed to tackle different aspects of influence campaigns, including both real and perceived threats of fake news, social media abuse, and election interference. Some governments are in the early stages of designing regulatory measures specifically for digital contexts so they can tackle issues related to the malicious use of social media. For others, existing legal mechanisms regulating speech and information are already well established, and the digital aspect merely adds an additional dimension to law enforcement.

Our research team conducted an analysis of proposed or implemented regulations and identified a number of interventions. Some measures target social media platforms, requiring them to take down content, improve transparency, or tighten data protection mechanisms. Other measures focus on civil actors and media organisations, on supporting literacy and advocacy efforts, and on improving standards for journalistic content production and dissemination. A third group of interventions target governments themselves, obligating them to invest in security and defence programs that combat election interference, or to initiate formal inquiries into such matters. Finally, a fourth group of interventions take aim at the criminalisation of automated message generation and disinformation.

There has long been a tension between allowing free speech to flourish while limiting the spread of undesirable forms of online content promoting hate, terrorism, and child pornography. Blocking, filtering, censorship mechanisms, and digital literacy campaigns have generally been the cornerstones of regulatory frameworks introduced in most countries, but with the growing challenges surrounding disinformation and propaganda new approaches for addressing old problems are flourishing. This paper provides an updated inventory of these new measures and interventions.

METHODOLOGY

We have created an inventory of the various government initiatives to tackle the multi-dimensional problems related to the malicious use of social media, such as the spread of dis/misinformation, automation and political bots, foreign influence operations, the malicious collection and use of data, and the weaponisation of attention-driven algorithms. We identified cases in three stages. First, we looked at the top-100 countries with the largest number of Internet users in 2016. Based on this list, we conducted an analysis using keywords related to social media manipulation, including fake news, political bots, online or computational propaganda, misinformation, and disinformation. We then searched for these terms in combination with our top 100 countries, as well as the keywords 'law', 'bill', 'legislation', 'act', and 'regulation' in order to identify instances of government responses to social media manipulation.

Using this approach, we identified a total of 43 cases that are either complete, in progress, or have been dismissed in which governments have introduced regulation in response to the malicious use of social media since 2016. The case studies were last updated in October 2018. We then drafted short case studies for each country to be reviewed by country-specific experts who ensured the accuracy of our information and provided additional country-specific information that could not be gleaned from non-English language bills or news sources. A summary of the various legal and regulatory mechanisms we identified can be found in Appendix 1.

We limited our analysis to legal and regulatory interventions designed in response to social media manipulation, and focused strictly on new or recently updated legal measures proposed in response to allegations of foreign interference in elections around the world, starting with the US election in 2016. For example, both Ghana and Gambia have long-standing legislation designed to tackle digital misinformation, but these countries are not included in our analysis since this legislation was not designed in response to the growing challenge of malicious use of social media. We have not reviewed measures where government legislative or executive branches have expressed interest in regulation, but still lack concrete proposals. We have also excluded pre-existing security-related solutions to disinformation or online propaganda, laws around hate speech, censorship, political campaigning or advertising, foreign intelligence, and other interventions that may have a digital aspect, but are not directly aimed at the growing proliferation of social media manipulation in democracies. Finally, we have not looked into regional or transnational initiatives, but have highlighted some of the more significant efforts initiated by the European Union, NATO, and other international organisations.

ANALYSIS OF MEASURES

Since 2016, 43 governments have proposed or implemented legal or regulatory responses to social media manipulation. A number of countries facing upcoming elections are at the forefront of addressing these issues. The following section explores the themes that have emerged from these various interventions. We have grouped the measures into four categories: (1) Measures Targeting Social Media Platforms, (2) Measures Targeting Offenders, (3) Measures Targeting Government Capacity, and (4) Measures Targeting Citizens, Civil Society and Media Organisations.

Measures Targeting Social Media Platforms

Content Takedowns by Social Media Platforms

Social media companies have become the central information highway for political news and information. Government-monitored removal, blocking, and filtering of illegal content online is a well-established practice in both democracies and authoritarian regimes. Whereas in the past, content takedown enforcement was managed through an Internet Service Provider, governments must now turn to social media companies to remove information deemed harmful. However, given their continued abuse and misuse by politically and economically motivated actors, social media companies have yet to implement sufficient countermeasures against the malicious use of their platforms.

A number of countries are in the process of approving legislation or have already established frameworks designed to address the spread of illegal or undesirable content on social media platforms. These measures typically put the onus on the platform to remove content or shutdown accounts with little government oversight and guidance. Countries such as Brazil, Germany, and South Korea have established or are proposing laws that require social media platforms to take down content deemed illegal by the state, or face hefty fines. However, our analysis concludes that some countries, such as Russia, Vietnam and Zimbabwe, are using similar legislation to legitimise further censorship of speech online. In democracies, there is also a risk of 'collateral censorship' where a lack of transparency around content moderation and blocking could lead to chilling effects in the digital public sphere.

Advertising Transparency

Political advertising in print and broadcast media is subject to tight regulations and standards that ensure the efficiency and

fairness of democratic processes. Several countries have laws regulating campaign spending, messages, scope, and timing. However, as campaigning has ventured into the online realm, with billions of dollars spent on advertising, engagement campaigns, and the curation of voter profiles, lawmakers have yet to extend the same scrutiny to digital contexts. Increasingly, regulators are becoming aware of issues surrounding the transparency of online advertising and are seeking to address them. Some proposed measures for online advertising transparency focus on improving transparency around the purchasers of advertising space and target audiences. The US, France, and Ireland require social network companies to collect and disclose information to users about who paid for an advert or piece of sponsored content, and to share information about the audience that advertisers target. Other efforts are designed to block foreign spending on domestic political campaigns. In addition, advertising giants such as Facebook and Google are engaging in self-regulatory measures, promising more transparency regarding advertising messages and their senders.

Data Protection

The malicious use of social media relies on highly data-driven targeting. Big data is leveraged to strengthen the impact and reach of messages using proprietary software, as well as tools and ad tech features available through private companies. The Cambridge Analytica revelations demonstrated that the data of millions of users has been used to disseminate manipulative news items and polarising information. Data breaches during the last two years at Google and Facebook have underscored the importance of data security, as the data of millions of users has been exposed. Despite these pressing challenges, only a few countries have chosen to implement new data protection measures to combat social media manipulation. Some national initiatives, such as Vietnam's data localisation law, which requires social media data to be stored within the borders of the state, can be used to further governmental control over citizen data. In Europe, the General Data Protection Regulation (GDPR), which came in to effect in May 2018, covers many of the data protection issues related to citizens based in the European Union. However, a global framework for data protection has yet to emerge, and even GDPR has gaps in coverage and enforcement that limit its effectiveness to address all problems associated with social media manipulation and data-driven targeting. For example, it remains unclear how social networks with international user bases will apply GDPR in local contexts. Following the implementation of GDPR, Facebook moved the data of 1.5 billion users out of Ireland so users outside of Europe cannot challenge privacy decisions under European law. And while GDPR helps protect elements of privacy for European citizens, it also has unintended consequences to the free flow of information where newspapers and other sources of information are no longer accessible to users based in Europe.

Measures Targeting Offenders

Criminalisation of Disinformation and Automation

In addition to requiring social media platforms to remove content, much proposed and implemented legislation concerns individuals who produce and/or share disinformation online. Several countries such as Egypt, Indonesia and Kuwait have strengthened government competencies to legally prosecute offenders, resulting in the criminalisation of posting and spreading disinformation online. Monetary fines and increased prison sentences are among the measures for deterring and prosecuting offenders. Other bills, such as in Ireland and California, do not merely prosecute the originators of online disinformation, but also those who maliciously disseminate and amplify it through automation. Rooting their countermeasures in various legal arguments surrounding national security, the disturbance of national order, hate speech, and the provision of false and misleading information, Australia, Indonesia, Ireland, Italy, Malaysia, and the Philippines are among the countries that rely on criminal penalties and fines for producing or sharing disinformation, or for creating and launching a bot campaign targeting a particular political issue. Instances of the misuse of these frameworks to crackdown on political dissidents, minorities, and human rights defenders have already taken place in Iran, Malaysia,[1] Russia, Saudi Arabia, and Tanzania.

Expanding the Definition of Illegal Content

The malicious use of social media is a relatively new phenomenon that takes advantage of the scale, targeting opportunities, and ease and speed of content creation and dissemination over the Internet and social media. Existing legislation is often viewed as inadequate in addressing new dynamics and content forms in our continuously evolving information ecosystem. This prompts regulators to revise bills, sharpen enforcement, and propose novel definitions of illegal content online. Thus far, it has been the world's democracies that have pioneered the redefinition of legal frameworks in connection to illegal content. Australian legislation authorises strict punishment for anyone found guilty of communicating information against the 'national interest', particularly with regard to false or distorted content. Germany's *Network Enforcement Act* explicitly extends the application of the German Criminal Code in cases where freedom of speech and constitutional values are in conflict. And France defers the legal interpretation of fake news and online content to its judiciary, whereby judges rule on prominent untruthful content on a case-by-case basis. Definitions around illegal forms of content in authoritarian countries are often wide-ranging to capture a diverse

1) Although Malaysia has since repealed its fake news law, the legislation was widely criticised by human rights activists for providing a new tool for censoring speech online.

collection of information, however, countries such as Saudi Arabia and Egypt have introduced new and even broader definitions of illegal content online.

Measures Targeting Citizens, Civil Society and Media Organisations

Media Literacy and Watchdogs

Countermeasures surrounding media literacy and watchdogs to fight social media manipulation generally focus on long-term educational and advocacy efforts. Tasked with improving public literacy in regard to digital information, practical skills in browsing the Internet for information, and evaluating the quality of content, many countries have begun funding long-term strategies to counter the malicious use of social media. For example, Croatia has funded a new media literacy initiative, rather than simply limiting the spread of malicious information online. Similarly, France is expanding the obligations of media watchdogs to improve public information literacy and exercise scrutiny over non-governmental institutions. Increasingly, these measures focus on improving public literacy, however there are still only a small number of initiatives to bring these skills to government institutions and public servants.

Media Accreditation and Journalistic Controls

Several governments have developed tighter controls over their national media in response to a changing media landscape and the spread of disinformation. Strategies, such as the United States' enforcement of the Foreign Agents Registration Act, seek to bolster quality journalism while improving transparency regarding information sources. However, other media accreditation strategies are deployed by restrictive regimes to exercise control over journalistic production of all content. For example, Iran and Tanzania have introduced or proposed bills to regulate journalistic research and production of content, resulting in ongoing public scrutiny in these countries regarding limitations on the freedom of the press.

Measures Targeting Government Capacity

Parliamentary Inquiries and Congressional Hearings

Parliamentary inquiries are a government tool often established in emergent or especially problematic political contexts. Inquiries are typically institutionalised within a country's legal framework, providing a committee with certain tasks and competencies. They are often the starting point for further regulation and action through the creation of policy briefs and recommendation documents. Following the Cambridge Analytica scandal, several countries launched parliamentary inquiries to understand the consequences of social media on democracy. In the UK the Digital, Culture, Media, and Sport Committee carried out an inquiry into the misinformation and digital manipulation of the public and its consequences. As a result of their initial report, the government is developing a

range of regulatory and non-regulatory initiates to address recommendations such as updating electoral laws for the digital age, protecting personal data, and empowering the electoral commission. In Singapore, the parliament unanimously voted to establish a Select Committee to tackle fake news; the committee has proposed a number of measures, including empowering government to make executive decisions about content moderation and disrupting the flow of digital advertising revenue. In Canada, the House of Commons has recently launched an investigation into data breaches and election integrity, and is carrying out research for its final report. In the United States, a series of congressional hearings have been investigating Russian interference in the 2016 election, the impact of the Cambridge Analytica scandal, and the political and market power of social media platforms in the digital era. At a regional level, the European Union also established a High-Level Expert Group that brought together government representatives, academics, and issue-area experts to put forward recommendations on combating the malicious use of social media, including media literacy, empowering journalists, and protecting the diversity and sustainability of the news ecosystem.

Security and Defence

Several governments have established cybersecurity and information security units within their militaries to address foreign interference in elections. Tasked with improving cybersecurity and citizens' rights online, these units engage in both the defence of informational infrastructure and strategic cyber warfare operations. As threats of social media manipulation and the spread of misinformation hit the global public agenda, some governments are mandating security and defence authorities to combat these threats, such as Australia's Election Integrity Task Force. Countermeasures include systematic observation of the online space, identifying offenders, analysing strategies of offense, reporting on problematic information as it rises to prominence, and debunking falsehoods. But security and defence operations remain opaque, with the scope of surveillance and intervention remaining unknown to the public. Brazil, the Czech Republic, Sweden, and Vietnam have introduced or proposed governmental authorities or military units tasked specifically with monitoring and combating various aspects of the malicious use of social media.

Monitoring and Reporting

Some government initiatives focus on monitoring the information ecosystem and providing users with portals to report misinformation. At a regional level, The East StratCom Task Force provides monitoring, training, and capacity building for disinformation campaigns that affect European Union institutions and member state governments. The G7 countries are also working on developing a Rapid Response Mechanism to combat disinformation and foreign interference in

elections. Italy provides one example of a national monitoring initiative where law enforcement has established a monitoring portal citizen can use to report instances of fake news for investigation in the run up to the next election.

Another form of monitoring initiative involves taxing citizens for using social media. For example, in Uganda the government has implemented a tax system to generate revenue and limit the amount of 'gossip' being shared on social media. Thus, to access certain online platforms, citizens are expected to pay approximately 200 Uganda shillings (0.05 EUR) per day to use the platforms.

CONCLUSION

There is no simple blueprint solution to tackling the multiple challenges presented by the malicious use of social media. In the current, highly-politicised environment driving legal and regulatory interventions, many proposed countermeasures remain fragmentary, heavy-handed, and ill-equipped to deal with the malicious use of social media. Government regulations thus far have focused mainly on regulating speech online—through the redefinition of what constitutes harmful content, to measures that require platforms to take a more authoritative role in taking down information with limited government oversight. However, harmful content is only the symptom of a much broader problem underlying the current information ecosystem, and measures that attempt to redefine harmful content or place the burden on social media platforms fail to address deeper systemic challenges, and could result in a number of unintended consequences stifling freedom of speech online and restricting citizen liberties.

As content restrictions and controls become mainstream, authoritarian regimes have begun to appropriate them in an attempt to tighten their grip on national information flows. Several authoritarian governments have introduced legislation designed to regulate social media pages as media publishers fine or imprison users for sharing or spreading certain kinds of information, and enforce even broader definitions of harmful content that require government control. As democratic governments continue to develop content controls to address the malicious use of social media in an increasingly securitised environment, authoritarian governments are using this as a moment to legitimise suppression and interference in the digital sphere.

In the future, we encourage policymakers to shift away from crude measures to control and criminalise content and to focus instead on issues surrounding algorithmic transparency, digital advertising, and data privacy. Thus far, countermeasures have not addressed issues surrounding algorithmic transparency and platform accountability: a core issue is a lack of willingness of the social media platforms to engage in constructive dialogue as technology becomes more complex. As algorithms and artificial intelligence have been protective of their innovations and reluctant to share open access data for research, technologies are blackboxed to an extent that sustainable public scrutiny, oversight and regulation demands the cooperation of platforms. Governments have put forward transparency requirements regarding political advertisements online, such as the Honest Ads act in the United States. While some platforms have begun to self-regulate, their self-prescribed remedies often fall short of providing efficient countermeasures and enforcement mechanisms.

Such legislation is important for addressing issues related to particular aspects of foreign interference in elections, such as the artificial inflation of hot button issues, or junk news designed to suppress voter turnout. However, many threats to the democratic process also come from within, and there is currently a lack of transparency regarding how misinformation spreads organically through likes and shares, and also around how political parties use social media to advertise to voting constituencies. Finally, while Europe's GDPR helps prevent some of the challenges arising from the malicious use of social media, and could have helped protect and remedy scandals such as Cambridge Analytica, data protection laws remain highly fragmented. Likeminded democratic governments should work together to develop global standards and best practices for data protection, algorithmic transparency, and ethical product design.

Appendix 1: Summary of National Legal and Regulatory Measures Taken by Governments in Response to the Malicious use of Social Media (2016–2018)

Country & Freedom House Score1 | **Measure** | **Challenge** | **Status1** | **Analysis** | **free** | **partly free** | **not free**

AUSTRALIA[2]
Draft Bill, Parliamentary Inquiry, Government Task Force (Electoral Integrity Task Force) | Foreign Interference, Content harmful to national interest | Proposed, Implemented, Implemented | Expanding Definition of Illegal Content, Media Accreditation, Security and Defence

AUSTRIA[3]
Court Ruling | Hate Speech | Implemented | Content Takedown

BELGIUM[4]
Government Task Force | Fake News | Implemented | Monitoring and Reporting

BELARUS[5]
Legal Amendment | Media Regulation | Implemented | Criminalisation

BRAZIL[6]
Government Task Force, Draft Bills | Fake News | Implemented, Proposed | Content Takedown, Criminalisation, Expanding Definition of Illegal Content, Security Defence and Monitoring

CAMBODIA[7]
Legislation | Fake news | Criminalisation

CANADA[8]
Parliamentary Inquiry | Foreign Interference, Data Protection | Implemented | Data Protection, Parliamentary Inquiry

CHINA[9]
Government Task Force | Content harmful to national interest | Implemented | Monitoring and Reporting

CROATIA[10]
Draft Bill | Hate Speech, Fake News | Proposed | Media Literacy and Watchdog Programs

CZECH REPUBLIC[11]
Government Task Force (Centre Against Terrorism and Hybrid Threats) | Foreign Interference, Content harmful to national interest | Implemented | Security and Defence

DENMARK[12]
Government Task Force and Media Literacy Campaign | Fake News, Foreign Interference, and Media Literacy | Implemented | Security and Defence, Media Literacy and Watchdog Programs

EGYPT[13]
Legislation | Fake news, Media Regulation | Implemented | Criminalisation, Media Accreditation

FRANCE[14]
Legislation (Proposition De Loi Relative a la lute contre les fausses informations) | Fake News, Foreign Interference, Advertising Transparency | Implemented | Expanding Definition of Illegal Content, Media Literacy and Watchdog Programs, Advertising Transparency

GERMANY[15]
Legislation (Network Enforcement Act) | Hate Speech | Implemented | Content Takedown, Expanding Definition of Illegal Content, Criminalisation

INDIA[16]
Draft Bill | Media Regulation | Dismissed | Media Accreditation

INDONESIA[17]
Draft Bill, Government Task Force (National Cyber and Encryption Agency), AI Solution | Fake News | Proposed, Implemented, Implemented | Criminalisation, Security and Defence

IRAN[18]
Regulation | Media Regulation, Fake News | Implemented | Media Accreditation

IRELAND[19]
Draft Bill (The Online Advertising and Social Media Transparency Bill) | Advertising Transparency, Bots and Automation | Proposed | Criminalisation, Advertising Transparency

ISRAEL[20]
Draft bill | Content harmful to democratic process | Dismissed | Content Takedown

ITALY[21]
Reporting Portal, Draft Bill (Regulations to Prevent the Manipulation of Online Information, Guarantee Web Transparency, and Incentivise Media Literacy) | Fake News, Content harmful to democratic process | Implemented, Proposed | Content Takedown, Criminalisation, Expanding Definition of Illegal Content

KENYA[22]
Legislation (The Computer and Cyber Crimes Bill 2018) | Fake News | Implemented | Content Takedown, Expanding Definition of Illegal Content

KUWAIT[23]
Legal Amendment | Fake News | Implemented | Criminalisation

MALAYSIA[24]
Legislation | Fake News | Repealed | Criminalisation, Expanding Definition of Illegal Content

NIGERIA[25]
Government Campaign | Media Literacy | Implemented | Media Literacy and Watchdog Programs

PHILIPPINES[26]
Draft Bill (The Anti-Fake News Act of 2017) | Fake News, Hate Speech, Defamation | Dismissed | Content Takedown, Criminalisation, Expanding Definition of Illegal Content

RUSSIA[27]
Legislation | Fake News, Media Regulation | Implemented | Content Takedown

SAUDI ARABIA[28]
Government Announcement | Fake News, Content harmful to national interests, Privacy | Implemented | Criminalisation

SINGAPORE[29]
Parliamentary Committee (Select Committee on Deliberate Online Falsehoods) | Fake News | Implemented | Parliamentary Inquiry

SPAIN[30]
Draft Bill | Fake News | Proposed | Data Protection

SOUTH AFRICA[31]
Draft Bill | Fake News | Proposed | Criminalisation, Expanding Definition of Illegal Content

SOUTH KOREA[32]
Draft Bill, Government Task Force | Fake News | Pending Amendments | Content Takedown, Security and Defence

SUDAN[33]
Draft Bill (Cybercrimes Law) | Fake News | Implemented | Criminalisation

SWEDEN[34]
Government Task Force (Swedish Civil Contingencies Agency and the Defence Commission) | Foreign Interference. Fake News | Implemented | Security and Defence

TAIWAN[35]
Educational Reform, Draft Bill (added clause to the Social Order Maintenance Act) | Fake News | Implemented, Proposed | Media Literacy and Watchdog Programs, Criminalisation

TANZANIA[36]
Legislation (Media Services Act) | Media Regulation, Fake News | Implemented | Content Takedown, Criminalisation, Media Accreditation

THAILAND[37]
Government Task Force | Fake News | Implemented | Monitoring and Reporting

TURKEY
Government Inquiry | Fake news | Implemented | Parliamentary Inquiry. Criminalisation

UGANDA[38]
Legislation (The Social Media Tax) | Fake News | Implemented | Monitoring and Reporting

UNITED KINGDOM[39]
Parliamentary Inquiry (DCMS), Government Task Force (National Security Communications Unit) | Foreign Interference, Fake News | Implemented, Implemented | Parliamentary Inquiry, Security and Defence

UNITED STATES[40]
Draft Bill (Honest Ads Act), Legislation (Countering Foreign Propaganda and Disinformation Act), Regulation (Foreign Agent Registration Act), Diplomatic (Expelling Diplomats), Senate Bill No. 1001 (State of California), New Media Literacy Law (State of California), Senate Committee Inquiries | Foreign Interference, Advertising Transparency, Bots and Automation, Media Literacy, Data Protection and Election Integrity | Proposed, Implemented, Implemented, Implemented, Implemented | Media Accreditation, Advertising Transparency, Parliamentary Inquiry, Data Protection, Security and Defence

VENEZUELA[41]
Legislation | Hate Speech | Implemented | Criminalisation

VIETNAM[42]
Draft Bill, Task Force (Force 47) | Fake News | Proposed | Data Protection, Security and Defence

ZIMBABWE[43]
Draft Bill | Fake news, Revenge Porn, Hate Speech | Proposed | Criminalisation

Endnotes

1 Freedom House Scores are based on the annual Freedom in the World Report Freedem House, "Freedom in the World 2018," January 13, 2018, https://freedomhouse.org/report/freedom-world/freedom-world-2018.

2 House of Representatives, "National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017" (2016), http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6022_ems_e4d3fac9-e684-40c4-b573-c000e7a32b03/upload_pdf/655771.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r6022_ems_e4d3fac9-e684-40c4-b573-c000e7a32b03%22; Michael McGowan, "Coalition's Security Laws 'Criminalise' Reporting, Media Companies Warn," *The Guardian*, January 24, 2018, sec. Australia news, http://www.theguardian.com/australia-news/2018/jan/25/coalitions-security-laws-criminalise-reporting-media-companies-warn; Amanda Meade, "Australia's Trust in Media at Record Low as 'fake News' Fears Grow, Survey Finds," *The Guardian*, 2018, https://www.theguardian.com/media/2018/feb/07/australias-trust-in-media-at-record-low-as-fake-news-fears-grow-survey-finds; Amy Remeikis, "Parliament to Launch Inquiry into 'fake News' in Australia," *The Sydney Morning Herald*, March 30, 2017, https://www.smh.com.au/politics/federal/parliament-to-launch-inquiry-into-fake-news-in-australia-20170330-gv9xwz.html.

3 Natasha Lomas, "Facebook Must Remove Hate Speech Posts, Austrian Court Rules," *TechCrunch* (blog), 2017, http://social.techcrunch.com/2017/05/08/facebook-must-remove-hate-speech-posts-austrian-court-rules.

4 De Standaard, "Minister De Croo Bindt Strijd Aan Met Fake News," *De Standaard*, February 5, 2018, http://www.standaard.be/cnt/dmf20180502_03492898; Government of Belgium, "Mijn Opinie - Mon Opinion," n.d., https://www.stopfakenews.be.

5 Radio Free Europe, "Belarus Passes Legislation Against 'Fake News' Media," *Radio Free Europe*, 2018, https://www.rferl.org/a/belarus-assembly-passes-controversial-fake-news-media-legislation/29291033.html; Committee to Protect Journalists, "Belarus Moves to Prosecute 'fake News,' Control the Internet," June 2018, https://cpj.org/2018/06/belarus-moves-to-prosecute-fake-news-control-the-i.php.

6 Melanie Ehrenkranz, "Brazil's Federal Police Says It Will 'Punish' Creators of 'Fake News' Ahead of Elections," *Gizmodo* (blog), 2018, https://gizmodo.com/brazil-s-federal-police-says-it-will-punish-creators-of-1821945912.

7 Asian Correspondent, "Cambodia Introduces Its Own 'Fake News' Law," *Asian Correspondent*, July 2018, https://asiancorrespondent.com/2018/07/cambodia-introduces-its-own-fake-news-law;
Khy Sovuthy, "Government to Tackle Fake News Frenzy," *Khmer Times*, July 5, 2018, https://www.khmertimeskh.com/50508265/government-to-tackle-fake-news-frenzy.

8 Kathleen Harris, "MPs Look for Ways to Fight 'fake News' in Wake of Mosque Shooting," *CBC*, February 2017, http://www.cbc.ca/news/politics/canada-fake-news-google-facebook-twitter-1.3961992.

9 Beijing Public Security Equipment, "Citizen Reporting Portal," 2017, http://www.81.cn/jubao;
Tim Crushing, "China Uses US Concern Over Fake News To Push For More Control Of The Internet," *Techdirt* (blog), November 2016, https://www.techdirt.com/articles/20161122/11501136116/china-uses-us-concern-over-fake-news-to-push-more-control-internet.shtml;
Rosie Perper, "China Created a Website for Vigilante Citizens to Report Leaks and Fake News," *Business Insider*, November 2017, http://www.businessinsider.com/china-military-crackdown-website-reports-fake-news-2017-11;
Catherine Wong, "China Will Boost Cyber Deterrence Powers, Vows President Xi Jinping," *South China Morning Post*, April 2016, http://www.scmp.com/news/china/policies-politics/article/1937224/china-will-boost-cyber-deterrence-powers-vows-president.

10 Tanja Ivancic, "The Government Is Preparing a Special Law to Punish Hate Speech on the Internet," *Vecernji*, January 2018, https://www.vecernji.hr/vijesti/vlada-priprema-poseban-zakon-kojim-ce-kaznjavati-govor-mrznje-na-internetu-1220126;
Peter Vidov, "The 'Lex Facebook' Could Easily Turn into Mass Censorship," *Faktograf*, January 2018, http://faktograf.hr/2018/01/16/vladin-lex-facebook-lako-bi-se-mogao-pretvoriti-u-masovnu-cenzuru.

11 Ministry of the Interior, "Centre Against Terrorism and Hybrid Threats - Terorismus a Měkké Cíle," 2018, http://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx.

12 Stop Fake, "Denmark's Defence Against Disinformation," *StopFake.Org* (blog), September 14, 2018, https://www.stopfake.org/en/denmark-s-defence-against-disinformation;
Tjekdek, "Danmark Får Ny Kommandocentral Mod Misinformation," *Tjekdek*, 2018,

https://www.mm.dk/tjekdet/artikel/danmark-faar-ny-kommandocentral-mod-misinformation;
Tjekdek, "Regeringens Plan for Håndtering Af Russisk Propaganda Er Lige På Trapperne," *Tjekdek*, 2018, https://www.mm.dk/tjekdet/artikel/regeringens-plan-for-haandtering-af-russisk-propaganda-er-lige-paa-trapperne.

13 Reuters, "Egypt Targets Social Media with New Law," July 17, 2018, https://www.reuters.com/article/us-egypt-politics/egypt-targets-social-media-with-new-law-idUSKBN1K722C;
Jared Malsin and Amira El Fekki, "Egypt Passes Law to Regulate Media as President Sisi Consolidates Power," *The Wall Street Journal*, July 16, 2016, https://www.wsj.com/articles/egypt-passes-law-to-regulate-media-as-president-sisi-consolidates-power-1531769232.

14 BBC, "Macron Announces 'fake News' Law," *BBC News*, January 2018, sec. Europe, http://www.bbc.co.uk/news/world-europe-42560688;
Angelique Chrisafis, "Emmanuel Macron Promises Ban on Fake News during Elections," *The Guardian*, January 2018, http://www.theguardian.com/world/2018/jan/03/emmanuel-macron-ban-fake-news-french-president;
James McAuley, "France Weighs a Law to Rein in 'Fake News,' Raising Fears for Freedom of Speech," *Washington Post*, January 10, 2018, sec. Europe, https://www.washingtonpost.com/world/europe/france-weighs-a-law-to-rein-in-fake-news-raising-fears-for-freedom-of-speech/2018/01/10/78256962-f558-11e7-9af7-a50bc3300042_story.html.

15 Patrick Beuth, "Heiko Maas: Auf Hass gezielt, die Meinungsfreiheit getroffen," *Die Zeit*, March 16, 2017, sec. Digital, http://www.zeit.de/digital/internet/2017-03/heiko-maas-gesetzentwurf-soziale-netzwerke-hass-falschnachrichten;
BMJV, "BMJV | Aktuelle Gesetzgebungsverfahren | Gesetz Zur Verbesserung Der Rechtsdurchsetzung in Sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG)," 2017, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html;
BMJV, "NetzDG - Gesetz Zur Verbesserung Der Rechtsdurchsetzung in Sozialen Netzwerken," September 2017, https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html;
Caroline Copely, "Merkel Fears Social Bots May Manipulate German Election," *Reuters*, November 2016, https://uk.reuters.com/article/uk-germany-merkel-socialbots/merkel-fears-social-bots-may-manipulate-german-election-idUKKBN13J1V2.

16 Funke, Daniel, "A Guide to Anti-Misinformation Actions around the World," Poynter, October 31, 2018, https://www.poynter.org/news/guide-anti-misinformation-actions-around-world."plainCitation":"Funke,
Daniel, "A Guide to Anti-Misinformation Actions around the World," Poynter, October 31, 2018, https://www.poynter.org/news/guide-anti-misinformation-actions-around-world."

17 Kanupriya Kapoor, "Indonesia's New Cyber Agency Looks to Recruit Staff of Hundreds," *Reuters*, January 2018, https://www.reuters.com/article/us-indonesia-cyber/indonesias-new-cyber-agency-looks-to-recruit-staff-of-hundreds-idUSKBN1EU15X;
Safrin La Batu, "Govt Deploys Artificial Intelligence to Combat Internet Hoaxes," *The Jakarta Post*, January 2018, http://www.thejakartapost.com/news/2018/01/31/govt-deploys-artificial-intelligence-to-combat-internet-hoaxes.html;
Kate Lamb, "Muslim Cyber Army: A 'fake News' Operation Designed to Derail Indonesia's Leader," *The Guardian*, March 2018, http://www.theguardian.com/world/2018/mar/13/muslim-cyber-army-a-fake-news-operation-designed-to-bring-down-indonesias-leader;
Arzia Tivany Wargadiredja, "Indonesia's Answer to Fake News Is a Threat to Free Speech," *Vice*, February 2018, https://www.vice.com/en_id/article/j5bq54/indonesias-answer-to-fake-news-might-be-a-threat-to-free-speech.

18 Mahsa Alimardani, "The Thin Line Between Political Censorship and Fighting Fake News in Iran," *Global Voices Advocacy* (blog), December 2016, https://advox.globalvoices.org/2016/12/08/the-thin-line-between-political-censorship-and-fighting-fake-news-in-iran.

19 Houses of the Oireachtas, "Online Advertising and Social Media (Transparency) Bill 2017" (2017), https://beta.oireachtas.ie/en/bills/bill/2017/150.

20 Raoul Wootliff, "Unwitting Israeli MKs Almost Pass Law Allowing Sweeping Internet Censorship," *Times of Israel*, n.d., https://www.timesofisrael.com/unwitting-israeli-mks-almost-passed-law-allowing-sweeping-internet-censorship.

21 Catherine Edwards, "Italy Debates Fines and Prison Terms for People Who Spread Fake News," *The Local*, February 2017, https://www.thelocal.it/20170216/italy-mulls-introducing-fake-news-fines;
Daniel Funke, "Italians Can Now Report Fake News to the Police. Here's Why That's Problematic.," *Poynter*, January 2018, https://www.poynter.org/news/italians-can-now-report-fake-news-police-heres-why-thats-problematic;
Angela Giuffrida, "Italians Asked to Report Fake News to Police in Run-up to Election," *The Guardian*, January 2018, http://www.theguardian.com/world/2018/jan/19/italians-asked-report-fake-news-police-run-up-election.

22 Jenny Gathright, "Kenya's Crackdown On Fake News Raises Questions About Press Freedom : The Two-Way," *NPR*, May 19, 2018, https://www.npr.org/sections/thetwo-way/2018/05/19/612649393/kenyas-crackdown-on-fake-news-raises-questions-about-press-freedom?t=1543400032758.

23 Arab Times, "Fine Upto KD 6,000 to Be Imposed for Incorrect or Fake News," May 14, 2018, http://www.arabtimesonline.com/news/fine-upto-kd-6000-to-be-imposed-for-incorrect-or-fake-news.

24 Daniel Funke, Alexios Mantzarlis, and Jane Elizabeth, "The Week in Fact-Checking: Malaysia Is Criminalizing Fake News," *Poynter*, April 2018, https://www.poynter.org/news/week-fact-checking-malaysia-criminalizing-fake-news; Parliament of Malaysia, "Anti-Fake News Bill 2018" (2018), https://drive.google.com/file/d/1H5fVRJJ46E5YXzvtnWNsxHlOqaSq0nYZ/view; Reuters Staff, "U.S. State Department Concerned by Malaysia's 'fake News' Bill," Reuters, April 2018, https://www.reuters.com/article/us-malaysia-election-fakenews-usa/u-s-state-department-concerned-by-malaysias-fake-news-bill-idUSKCN1HA27D.

25 Evelyn Okakwu, "Nigerian Govt Launches Campaign against 'Fake News,'" *Premium Times*, July 11, 2018, https://www.premiumtimesng.com/news/more-news/275846-nigerian-govt-launches-campaign-against-fake-news.html.

26 Joel Villanueva, "Bill of the Anti-Fake News Act of 2017," Pub. L. No. S.B. No. 1492 (2017), http://www.aseanlip.com/philippines/ip/legislation/bill-of-the-antifake-news-act-of-2017/AL18286.

27 Reporters Without Borders, "Russian Bill Is Copy-and-Paste of Germany's Hate Speech Law," *Reporters Without Borders: For Freedom of Information* (blog), July 2017, https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law.

28 Matt Novak, "Saudi Arabia Threatens Anyone Spreading 'Fake News' Online with 5 Years in Prison, Heavy Fines," *Gizmodo* (blog), October 15, 2018, https://gizmodo.com/saudi-arabia-threatens-anyone-spreading-fake-news-onlin-1829749930.

29 Ng Jun Sen, "Select Committee to Examine Fake News Threat in Singapore," *The Straits Times*, January 2018, https://www.straitstimes.com/politics/select-committee-to-examine-fake-news-threat; Chan Luo Er, "New Laws on Fake News to Be Introduced next Year: Shanmugam," *Channel News Asia*, June 2017, https://www.channelnewsasia.com/news/singapore/new-laws-on-fake-news-to-be-introduced-next-year-shanmugam-8958048; Parliament Of Singapore, "Select Committee on Deliberate Online Falsehoods - Causes, Consequences and Countermeasures," Parliament Of Singapore, January 2018, https://www.parliament.gov.sg/sconlinefalsehoods; Ang Yiying, "Tackling the Real Issue of Fake News," *The Straits Times*, April 2018, https://www.straitstimes.com/opinion/tackling-the-real-issue-of-fake-news; Yiying.

30 Miquel Alberola, "Fake News: Spanish Socialists Propose Measures to Curb Online Fake News | In English," *EL PAÍS*, April 2018, https://elpais.com/elpais/2018/04/04/inenglish/1522825133_619847.html.

31 Agence France-Presse, "South Africa Weighs Social Media Measures to Fight Fake News," *Rappler*, March 2017, http://www.rappler.com//technology/social-media/163328-south-africa-measures-fight-fake-news; National Assembly of South Africa, "Cybercrimes and Cybersecurity Bill" (2016), http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf.

32 Seo Jung-Hwan, "민주당 댓글조작·가짜뉴스법률대책단, 가짜뉴스 유포자 45건을 추가 고소," *Hankyung*, March 2018, http://www.hankyung.com/news/app/newsview.php?aid=201803126591i; National Assembly of South Korea, "Bill Information System," 2018, http://likms.assembly.go.kr/bill/main.do; Doug Tsuruoka, "Asia Ahead of US in Passing Laws against Social Media Abuse," *Asia Times*, March 2018, http://www.atimes.com/article/asia-ahead-us-passing-laws-social-media-abuse.

33 Freedom House, "Sudan Country Profile," 2016, https://freedomhouse.org/report/freedom-net/2016/sudan; SMEX, "Do New Sudanese Laws Regulate Digital Space or Limit Freedom of Expression?," *SMEX* (blog), July 23, 2018, https://smex.org/do-new-sudanese-laws-regulate-digital-space-or-limit-freedom-of-expression.

34 Michael Birnbaum, "Sweden Is Taking on Russian Meddling Ahead of Fall Elections. The White House Might Take Note.," *Washington Post*, February 2018, https://www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html; The Local, "Sweden to Create New Authority Tasked with Countering Disinformation," *The Local*, January 2018, https://www.thelocal.se/20180115/sweden-to-create-new-authority-tasked-with-countering-disinformation.

35 Nicola Smith, "Schoolkids in Taiwan Will Now Be Taught How to Identify Fake News," Time, April 6, 2017, http://time.com/4730440/taiwan-fake-news-education.

36 Abdi Latif Dahir, "You Now Have to Pay the Government over $900 a Year to Be a Blogger in Tanzania," *Quartz* (blog), April 2018, https://qz.com/1248762/tanzania-social-media-and-blogging-regulations-charge-to-operate-online; Silvia Morales, "New Media Bill Threatens Press Freedom in Tanzania," *International Press Institute* (blog), November 2016, https://ipi.media/new-media-bill-threatens-press-freedom-in-tanzania; Daniel Mumbere, "Tanzania Cyber Law Introduces $900 Fees for Bloggers, Compulsory Passwords | Africanews," *Africa News*, April 2018,

http://www.africanews.com/2018/04/12/tanzania-cyber-law-introduces-900-fees-for-bloggers-compulsory-passwords;
United Republic of Tanzania, "The Media Services Act 2016," Pub. L. No. ISSN 0856-35X, 97 36 (2016), http://parliament.go.tz/polis/uploads/bills/1474021216-A%20BILL%20-%20%20%20THE%20MEDIA%20SERVICES%20ACT,%202016.pdf.

37 Shawn Lim, "Thailand Launches 'Media Watch' App to Combat Fake News," *The Drum*, December 2017, http://www.thedrum.com/news/2017/12/01/thailand-launches-media-watch-app-combat-fake-news.

38 Agence France-Presse, "Social Media Use Taxed in Uganda to Tackle 'Gossip,'" *The Guardian*, June 1, 2018, https://www.theguardian.com/world/2018/jun/01/social-media-use-taxed-in-uganda-to-tackle-gossip.

39 House of Commons Select Committee, "'Fake News' Inquiry Launched," UK Parliament, January 2017, https://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news-parliament-2015/fake-news-launch-16-17;
Peter Walker, "New National Security Unit Set up to Tackle Fake News in UK," *The Guardian*, January 2018, http://www.theguardian.com/politics/2018/jan/23/new-national-security-unit-will-tackle-spread-of-fake-news-in-uk.

40 Lauren Gambino, Sabrina Siddiqui, and Shaun Walker, "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking," *The Guardian*, December 2016, https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack;
Amy Klobuchar, "Honest Ads Act," Pub. L. No. S.1989 (2017), https://www.congress.gov/bill/115th-congress/senate-bill/1989/text;
Natalka Pisnia, "Why Has RT Registered as a Foreign Agent with the US?," *BBC News*, November 2017, http://www.bbc.co.uk/news/world-us-canada-41991683;
Rob Portman, "Countering Information Warfare Act of 2016," Pub. L. No. S.2692 (2016), https://www.congress.gov/bill/114th-congress/senate-bill/2692/related-bills;
Chase Purdy, "California Has a Plan to Police Facebook," *Quartz* (blog), March 2018, https://qz.com/1234829/california-has-a-plan-to-police-facebook.

41 Mia Alberti, "Venezuela Media Law: 'Threat to Freedom of Expression'?," *Al Jazeera*, November 2017, https://www.aljazeera.com/news/2017/11/venezuela-media-law-threat-freedom-expression-171117180846540.html;
Richard Gonzales, "Venezuela Constituent Assembly Cracks Down On Media," *NPR*, November 2017, https://www.npr.org/sections/thetwo-way/2017/11/08/562954354/venezuela-constituent-assembly-cracks-down-on-media.

42 Dien Luong, "Vietnam Wants to Control Social Media? Too Late.," *The New York Times*, November 2017, https://www.nytimes.com/2017/11/30/opinion/vietnam-social-media-china.html;
Ministry of Public Security, "Luật An Ninh Mạng" (2017), http://duthaoonline.quochoi.vn/DuThao/Lists/DT_DUTHAO_LUAT/View_Detail.aspx?ItemID=1382&LanID=1497&TabIndex=1;
Reuters, "Vietnam Unveils 10,000-Strong Cyber Unit to Combat 'Wrong Views,'" *Reuters*, April 2018, https://www.reuters.com/article/us-vietnam-security-cyber/vietnam-unveils-10000-strong-cyber-unit-to-combat-wrong-views-idUSKBN1EK0XN;
Reuters, "Vietnam's President Calls for Tougher Internet Controls," *Reuters*, August 2017, https://www.reuters.com/article/us-vietnam-internet/vietnams-president-calls-for-tougher-internet-controls-idUSKCN1B00JW.

43 The Parliament and the President of Zimbabwe, "Cybercrime and Cybersecurity Bill 2017" (2017), https://t792ae.c2.acecdn.net/wp-content/uploads/2017/08/CYBERCRIME-AND-CYBERSECURITY-BILL2017.pdf.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org