LAW LIBRARY
LIBRARY OF CONGRESS

Government Responses to Disinformation on Social Media Platforms

Argentina • Australia •Canada • China • Denmark
Egypt • European Union • France• Germany
India • Israel • Mexico • Russian Federation
Sweden • United Arab Emirates
United Kingdom

September 2019

Report for Congress
LL File No. 2019-017919

The Law Library of Congress, Global Legal Research Directorate
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Comparative Summary

Ruth Levush
Senior Foreign Law Specialist

Concerns regarding the impact of viral dissemination of disinformation on democratic systems of government, on political discourse, on public trust in state institutions, and on social harmony have been expressed by many around the world.[1] These concerns are shared by countries with advanced economies as well as those with emerging and developing economies.[2]

The term "disinformation" as used in this report refers to "false information deliberately and often covertly spread . . . in order to influence public opinion or obscure the truth."[3] Disinformation for this purpose,

> does not cover issues arising from the creation and dissemination online of illegal content (notably defamation, hate speech, incitement to violence) . . . , nor other forms of deliberate but not misleading distortions of facts such a [sic] satire and parody.[4]

The use of technological tools and techniques, including bots, big data, trolling, deep-fakes, and others, enables those intending to manipulate public opinion by spreading false, inaccurate, or misleading information, to reach targeted and potentially endless audiences. The use of technology in influencing campaigns becomes harder to spot when individuals or foreign adversaries anonymously facilitate the creation of internal tensions within the country. The inability to trace sources further enables dissemination of political ads by foreign or domestic sources in violation of campaign financing rules, in countries where such rules apply.

While the dangers associated with the viral distribution of disinformation are widely recognized, the potential harm that may derive from disproportional measures to counter disinformation should not be underestimated. Unlimited governmental censorship of online communications; an expansive definition of what constitutes "disinformation"; broad application of emergency powers to block content based on grounds of national or public security; draconian penalties for alleged offenders without the ability to present an effective defense; and strict enforcement of defamation laws in the absence of journalistic defenses are just a few examples of potential threats to the principle of free speech and the administration of the rule of law posed by overreaching regulations concerning disinformation.

---

[1] See, e.g., National Endowment for Democracy, *Issue Brief: How Disinformation Impacts Politics and Publics* (May 29, 2018), https://perma.cc/UGZ2-ETBG.

[2] Conor Sanchez, *Misinformation Is a Threat to Democracy in the Developing World*, Council on Foreign Relations (Jan. 29, 2019), https://perma.cc/S4CB-GK8M.

[3] See, e.g., "Disinformation," Merriam-Webster, https://perma.cc/9TY2-5D6J.

[4] Press Release, European Commission, Final Report of the High Level Expert Group on Fake News and Online Disinformation (Mar. 12, 2018) (describing the term for purposes of the European Commission report), https://perma.cc/Y4TC-WBR8.

This report is composed of individual surveys of the European Union (EU) and fifteen selected countries from around the globe. The countries surveyed vary geographically, culturally, in their systems of government, and in their commitment to democratic principles of governance, which include protections for freedom of expression, the right to privacy, and transparency and oversight of governmental actions, among other things. The surveys were prepared by the foreign law specialists and analysts of the Law Library of Congress's Global Legal Research Directorate based on primary and secondary sources available in the Law Library of Congress's collections, legal databases to which it subscribes, and open sources.

The following summary of the report's findings is based on more expansive information contained in the individual surveys. It addresses reported instances of alleged disinformation and highlights governmental responses to challenges posed by the spread of disinformation on social media platforms.

I. Reported Instances of Online Distribution of Disinformation

The dissemination of disinformation to create tensions in society, to further political agendas, or to delegitimize political opponents has been utilized by foreign as well as domestic actors.

A. Foreign Intervention

The spread of disinformation on social platforms has been considered a threat to national security and to democratic systems of government in a number of the surveyed countries. In particular, concerns ahead of national elections were expressed in **Argentina**, **India**, **Israel**, **Mexico**, and **Sweden**.

Specific instances of disinformation by **Iran** were detected by Facebook. In a January 31, 2019, press release, Facebook announced that it had removed 783 specific pages, groups, and accounts for engaging in coordinated inauthentic behavior tied to that country. There were multiple sets of activity, according to Facebook, each localized for a specific country or region, including the following countries: **Afghanistan**, **Albania**, **Algeria**, **Bahrain**, **Egypt**, **France**, **Germany**, **India**, **Indonesia**, **Iran**, **Iraq**, **Israel**, **Libya**, **Mexico**, **Morocco**, **Pakistan**, **Qatar**, **Saudi Arabia**, **Serbia**, **South Africa**, **Spain**, **Sudan**, **Syria**, **Tunisia**, the **US**, and **Yemen**. According to Facebook,

> [p]age administrators and account owners typically represented themselves as locals, often using fake accounts, and posted news stories on current events. This included commentary that repurposed Iranian state media's reporting on topics like **Israel-Palestine** relations and the conflicts in **Syria** and **Yemen**, including the role of the **US**, **Saudi Arabia**, and **Russia**. Some of the activity dates back to 2010. Although the people behind this activity attempted to conceal their identities, our manual review linked these accounts to **Iran**.[5]

In 2019, CBC/Radio **Canada** conducted a multi-year analysis of 9.6 million tweets from Twitter accounts that have since been deleted and found that approximately 21,600 tweets were from troll accounts suspected to have originated from **Russia**, **Iran**, and **Venezuela**, targeting Canadians

[5] *Removing Coordinated Inauthentic Behavior from Iran*, Facebook Newsroom (Jan. 31, 2019) (emphasis added), https://perma.cc/ K2HX-D4CE.

with messages critical of Canadian pipeline projects and Canada's policies on immigration and refugees.

A 2017 **Danish** Defense report points to what it identified as a **Russian** general policy, ever since the Cold War, that internal tensions within a country increase the level of influence that Russia exercises over the rest of the world. The report notes that the use of technology in influencing campaigns becomes harder to spot as statements on social media appear to have no state affiliation and the Russian origin has been disguised. The Danish Defense also notes that other non-state actors, such as militant Islamists, use social media for propaganda purposes.

Strong indications that **Russia** attempted to interfere with the **French** presidential election of 2017 allegedly included the last-minute release of a massive amount of leaked emails from the campaign of then-candidate Emmanuel Macron, among which were embedded fake emails.

B. Allegations of Domestic Disinformation

In **Australia**, during the lead up to the May 2019 federal election, one political party asked Facebook to remove posts containing false information, claiming that the party planned to introduce a "death tax."

In **Germany,** a criminal complaint was filed in 2016 by a Green Party politician against the operators of a Facebook page and unknown persons for displaying her picture with a fake quote expressing compassion for a refugee who killed a student.

As compared with allegations made by politicians or political parties in countries like Australia and Germany, claims of the online spread of rumors, fake news, and disinformation were made by the governments of **China, Egypt, Russia, and the United Arab Emirates**. Such claims were made regarding content viewed by authorities as objectionable. The criteria for determining what constitutes objectionable information may not always be obvious.

In **China**, despite the strict regulation of the media and the internet, 6.7 million reports of illegal and false information, often referred to as "rumors," were allegedly disseminated in a single month in July 2018.

In June 2019, the undersecretary of the General Directorate of Information and Relations at the **Egyptian** Interior Ministry alleged that there were around 4 to 6 million pages circulating misinformation on social media accounts targeting Egyptians. In 2018, the Egyptian President asserted that the Egyptian government had identified around 21,000 "rumors" that were circulated on social media over a three-month period that year. According to the Communication and Information Technology Committee in the Egyptian Parliament, 53,000 false rumors had allegedly been spread in Egypt in just sixty days in 2017.

Russian law defines "fake news" broadly to include "socially significant" disinformation that among other things might cause mass violations of public order or public security, or interfere with vital state interests such as transportation, social infrastructure, credit institutions, or modes of communication or industry and energy enterprises. A 2019 court decision in a case involving a **Russian** political activist addresses the required elements for conviction under Russian "anti-

fake-news" laws. The activist had reportedly been charged with spreading disinformation on her social media account for publicizing an unauthorized protest against the selection of a site in a Russian city for waste disposal. Dismissing the case, the court held that the charges did not specify which words published by the activist were false and the criteria by which the determination regarding their falsehood was made. The court declared that violating the procedure for organizing a public event and publicizing the event, by themselves, are not violations of the anti-fake-news law.

In the **United Arab Emirates** the posting of a picture of a car parked across two disability parking spaces was the ground for conviction of an Australian woman under a law that prohibits online publication of information, news, statements, or rumors designed to damage the interests, reputation, prestige, and stature of the state or any of its institutions, its officials, or national symbols. In another case, two women who posted a video on social media of a woman of African origin carrying an Emirati child, claiming the child had been abducted, were similarly charged with disseminating false information on social media, after the police determined the child was taken by his nanny per his mother's instructions. A ten-year sentence was reportedly imposed in a third case on a person convicted of using social media to spread unidentified false stories that harmed the country's reputation and its foreign policies.

II. Cybersecurity

Many of the countries surveyed operate cybersecurity measures to protect governmental computerized systems and software applications against communications containing threats to national security, including, but not limited to, disinformation. For example, the **Israel** National Cyber Directorate, which reports directly to the Prime Minister, is tasked with monitoring and preventing such threats from materializing.

The **United Kingdom** government announced that it would "significantly expand" the National Security Communications Team (NSCT). A spokesperson for then Prime Minister Theresa May outlined that the NSCT would be tasked with combating disinformation by state actors and others in order to systematically deter adversaries and protect national security.

Some countries have established special task forces to guard against cyberattacks and interference in elections. In **Australia**, the Australian Electoral Integrity Assurance Taskforce was established in 2018 with the mission of protecting Australia's democracy against malicious cyber activity, electoral fraud, foreign interference, and disinformation. The Taskforce is led by the Department of Home Affairs, with involvement from the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP).

A similar interdepartmental task force against disinformation was established in **Denmark** in 2018, whereby the Danish Security Intelligence Service and the Danish Defense Intelligence Service de facto created a command center with the purpose of countering disinformation from foreign sources. The initiatives provided that the agencies should collaborate in ensuring the conduct of threat and vulnerability assessments in relation to the election; focus on threats posed by potential foreign influence; and offer all political parties eligible to be elected to Parliament counseling on the risk of foreign influence in relation to the upcoming parliamentary elections, including cyberattacks, and on the options for countering such influence and attacks.

Two **French** government agencies, the National Commission for the Control of the Electoral Campaign for the Presidential Election and the National Cybersecurity Agency, served a key role in countering alleged **Russian** efforts to interfere in the French presidential election of 2017.

The **Canadian** Security and Intelligence Threats to Elections Task Force has similar responsibilities for preventing covert, clandestine, and criminal activities from interfering with or influencing the electoral process.

III. Mandatory Requirements for Transparency and Accountability

A. Licensing and Ongoing Monitoring

A high level control over social media activities exists in **China,** the **Russian Federation**, and the **United Arab Emirates**. **China** requires social media platforms to be licensed, and their users must register their real names and other identity information with service providers. The **United Arab Emirates** further requires licensing by its National Media Council for electronic advertisements and for any other electronic activity deemed by authorities to be appropriate.

Russian law authorizes the Roskomnadzor, the federal executive body overseeing mass media and information technology, to create and maintain a state registry of banned information resources in Russia. It also provides for full access by investigative bodies to the hardware and software of resource providers, and authorizes the Roskomnadzor to demand that a provider fully identify the owner of its hardware and software. Additionally, owners of news aggregators (who must be Russian physical or legal persons) are required to verify the validity of socially significant facts considered fake news and prevent the use of the news aggregator to conceal, falsify, or disseminate such news.

To eliminate alleged disinformation circulating through social media outlets and combat extremist ideology, the **Egyptian** government has announced that it is taking effective steps toward creating an Egyptian local version of Facebook, which will presumably allow authorities to have control over messages deemed unlawful. A state-wide version of Facebook already exists in **China**, where the biggest social media platform WeChat, operated by Tencent, is used.

B. Transparency of Political Ads

As compared with the above sample of high-level media control, varied levels of transparency requirements for online communications on social platforms were identified in other surveyed countries. Such requirements are often limited to relevant periods of electoral campaigns. A recent amendment to **Argentinian** law on financing of political parties, for example, includes specific measures aimed at enhancing the transparency and accountability of online political advertising, such as requiring those ads to be paid by credit card with full disclosure of the purchaser's identity and the registration of political parties' social media accounts. Additionally, at the time they report their digital platform campaign expenses, political parties are required to submit all audiovisual material pertaining to the political campaign that is available on the internet, social media networks, messaging, and any other digital platform.

Australia requires all paid electoral advertising, including advertisements on social media, to be authorized and to contain an authorization statement. Authorization statements must also be included in political communications by those subject to the Commonwealth electoral funding and financial disclosure regime. These include candidates; parties; political campaigners; organizations or persons who have incurred significant electoral expenditure; and organizations or persons who have donated more than a predetermined disclosure threshold to a political party, political campaigner, or third party. Additional disclosure requirements apply to people and entities who undertake communications activity in Australia on behalf of a foreign principal for the purpose of political or governmental influence, or who produce information or material on behalf of a foreign principal for the purpose of being communicated or distributed to the public.

Canadian law requires online platforms to keep and maintain a digital registry of all regulated ads related to federal elections, indicating the names of agents who authorized them and any partisan advertising and election advertising that was published on the platform during election periods. Political ads must be kept in the registry for a period of two years following an election; information concerning ads must be kept by platform operators or owners for an additional five years.

Israel's Central Election Committee has extended transparency requirements previously applicable by legislation to printed advertisements to advertisements disseminated on the internet. These requirements apply to the disclosure of identifying information of the person, candidate, or candidates' list on behalf of whom the election advertisement was published.

The **European Commission** issued a recommendation ahead of the 2019 European Parliament elections calling on European Union Member States to promote active disclosure of who is behind paid, online political advertisements and communications during electoral campaigns.

Extensive requirements for the transparency of political content have been adopted in **France**, an EU Member. Accordingly, online platforms with at least five million unique visitors per month must provide users with information on the identification of the persons or organizations that bought paid content related to topics of national interest. Public disclosure requirements are also imposed under French law on online platforms that are paid beyond a certain amount for sponsored content. Additionally, online platform operators that use algorithms to recommend, sort, or reference content related to topics of national interest are required to publish statistics for every item of content: the share of direct access, the share of access through the platform's recommendation, sorting and referencing algorithms, and the share of access through the platform's internal search function. These statistics are to be published online and made accessible to everyone.

France and **Germany** require online platforms to establish an easily accessible and visible way for users to flag false information, with **Germany** further requiring responses to complaints to be provided without undue delay. More expansive requirements are currently under consideration in **Germany** that would require media intermediaries to identify social bots and impose a general duty for all electronic media to clearly identify persons posting political, ideological, or religious advertisements.

The identification of the social media accounts of candidates and the preapproval of political ads transmitted via social media websites are required under **Indian** law. Expenditures on advertisements on social media must be reported in India as well as in some of the other countries surveyed.

IV. Blockage or Removal of Posts

Blockage or removal of illegal content may be required under the laws of a number of countries surveyed on grounds that do not necessarily view such content as disinformation. Such requirements apply with regard to "abhorrent violent material" in **Australia**. Under **Danish** law, public access to websites may be blocked if there are grounds to believe its content promotes or sponsors terrorism. **German** law authorizes blockage or removal of posts that seek to disseminate propaganda material or use symbols of unconstitutional organizations; encourage the commission of a serious violent offense; endanger the state; and advocate the commission of treasonous forgery, public incitement to crime, and incitement to hatred.

Similar grounds for blockage and removal may be imposed under **United Arab Emirates** laws that apply to online publications that promote rioting, hatred, racism, sectarianism, or damage to or disturbances of the public order. Additional grounds for blockage and removal extend under this country's law to the publication of content that harms national unity or national symbols; public morals; or the reputation, prestige, or stature of the state or any of its institutions, its royal family, or high public officials.

Expansive grounds for blockage or removal are found under **Indian** law when the central government determines that it is necessary or expedient to do so based on the interest of India's sovereignty, integrity, security, foreign affairs, or public order. In addition to blockage or removal, the Indian government may authorize internet shutdowns to prevent danger to human life, health, or safety, or the disruption of public peace. Draft rules proposed in 2018 would further require intermediaries to proactively monitor and filter unlawful content and provide for the traceability of users. Recommendations for the introduction of a similar duty of care have been expressed in several government reports in the **United Kingdom**.

Extensive requirements are already in place in **China**, where network operators must monitor, report, and remove from their platforms content deemed by authorities to be false and capable of endangering the state economy, social order, and national security.

Russian law authorizes the blockage of information found to constitute fake news, as well as of content that offends human dignity and public morality or shows obvious disrespect for the Russian Federation, its Constitution, or its legal authorities.

As compared with the general authorization of blockage or removal of objectionable content under the laws of the abovementioned countries, blockage or removal in **France** is limited in duration and limited to the election period, and may only be authorized by a judge. Judicial authorization may only be granted based on a determination that such measures are proportional and necessary to stop the deliberate, artificial, or automatic and massive dissemination of fake or misleading information online. Additionally, France's main regulatory agency for radio and television broadcasting may suspend the broadcasting license of an operator controlled by or

under the influence of a foreign state if, during an election period, it broadcasts false information that could affect the election results.

V. Criminal Sanctions for Spreading Disinformation

Criminal sanctions and penalties extending to imprisonment and fines are available in a number of surveyed countries for offenses involving the spread of misinformation to further unlawful objectives, such as defamation, hate speech, terrorism, or incitement to violence, or the publication of abhorrent violent material.

In view of rising levels of foreign influence campaigns, a 2019 **Danish** amendment criminalizes the dissemination of disinformation that "aids or enables" a foreign state actor to influence public opinion in Denmark. The amendment imposes a maximum penalty of twelve years' imprisonment for offenses carried out in connection with Danish or EU parliamentary elections. Comments and posts published on Facebook or other social platforms do not qualify, as social media platforms are generally not considered a foreign power. Although the use of bots in connection with prohibitions on foreign influence activities was referenced in the amendment's draft bill on foreign interference, the amendment did not extend so far as to prohibit their use.

The making of false statements about a candidate's criminal record, citizenship, place of birth, education, professional qualifications, or membership in a particular group, as well as the candidate's withdrawal from an election, are prohibited under **Canadian law**. Platform operators or owners can also be prosecuted for knowingly selling election advertising to non-Canadians. These crimes are hybrid offenses subject to fines and imprisonment that vary depending on whether they are prosecuted summarily or based on an indictment.

Punitive measures are prescribed under **Russian** law for disseminating fake news and for the online publication of content that disrespects state symbols, the Constitution, and Russian Federation authorities. The spreading of fake news is usually punishable by fines at a rate that depends on whether individuals, legal persons, or officials are involved, with repeat offenders being subject to up to fifteen days' administrative arrest.

Severe penalties are imposed in **China**, **Egypt**, and the **United Arab Emirates** for disinformation deemed to be affecting state interests. Spreading false information that seriously disturbs public order through an information network or other media constitutes a crime punishable by up to seven years in prison in **China**. In **Egypt,** the deliberate spreading of false information or rumors abroad about the internal conditions of the country in a way that might weaken the country's financial credibility or harm the country's national interests is punishable by six months to five years of imprisonment and a fine. Similarly, in the **United Arab Emirates**, the publication of content designed to endanger the national security and the higher interests of the state or to disturb the public order is punishable by imprisonment and a fine.

VI. Other Government Actions

Digital educational programs including the issuance of handbooks and social media advertising campaigns to raise awareness of the responsible and critical use of online election information are offered in **Argentina**, **Australia**, **Canada**, **Denmark**, **France**, **Germany**, **Israel**, the **United Arab Emirates**, and the **United Kingdom.** These programs are designated for government employees as well as the public at large.

Additional government actions against the spread of disinformation include the adoption of a special digital charter and implementing strategies by the **Canadian** government, among others, to inform candidates, organizations, and elections officials if they have been the known targets of an attack.

European Union institutions fund projects for monitoring risks and mapping violations to media pluralism across Europe. They further fund cross-border investigative journalism and support journalists under threat. A special body, the East StratCom Task Force, was created within the European External Action Service with the expressed mission of "address[ing] Russia's ongoing disinformation campaigns." The task force has set up an "EU v Disinformation" webpage, which functions as an EU-wide rapid alert system, facilitates the sharing of insights related to disinformation campaigns, and coordinates responses. The system is based on open-source information and also draws expertise from academia, fact-checkers, online platforms, and international partners. The EU is also funding a joint, EU-wide network for fact-checkers, as well as projects in the field of media freedom and pluralism.

Mechanism for citizens' reporting were identified in Israel and in Egypt. **Israel**'s central election commission website provides contact numbers for its service centers for all complaints and issues related to elections and voting. It further provides contact numbers for the police hotlines, as the police will also be responding to calls regarding computer crimes. Other reporting options to complain about any attempts to manipulate voters through fake profiles and the like include the National Center for Cyber Incidents and Information Security.

The **Egyptian** Public Prosecutor has announced the creation of a new hotline for citizens to file complaints against false news posted by media outlets or by individuals on social media networks.

To counter online "rumors," **China** has launched a platform to broadcast "real" news sourced from state-owned media, party-controlled local newspapers, and various government agencies.

VII. Media Coordination and Initiatives

The **European Union** and many of the surveyed countries have entered into agreements with online media platforms to cooperate in preventing the spread of disinformation. Such agreements may include flagging or certification for political ads, voluntarily informing users of upcoming elections, monitoring suspicious or illegal activities during election periods, and vetting and rating stories published on their platforms.

In **Australia**, the Electoral Commission established protocols with Facebook and Twitter relating to removing or blocking posts that breach electoral advertising laws, or reporting details of their creators to the Commission. Facebook also committed to banning foreign-funded political advertisements and to cracking down on fake accounts during the **Australian** federal election period. Twitter, on its part, announced that it would require political campaign advertisers in **Australia** to apply for certification, meet certain profile requirements, and comply with applicable laws.

Facebook, Google, Twitter, and Mozilla, as well as advertising trade associations, have signed the **European Union** Code of Practice on Disinformation (CPD), which requires, among other things, that advertisements should be clearly distinguishable from editorial content. In consideration of the CPD, Google has included policies and information that specifically apply to the EU, such as an advertiser verification requirement for election ads in the European Union. Twitter has established a general certification process for the EU involving particular identification, disclosure, eligibility, and reporting requirements. Once certified, political campaign advertisers will be prompted to use "paid for by" disclaimers. The certification process appears to differ, however, based on the country-specific approach, and does not apply to **France**, where Twitter has announced that political campaigning ads will not be permitted.

Facebook requires political parties and election candidates to register on the platform before publishing content seeking votes. In addition, sponsored content is required to show who paid for it. Facebook **Germany**, for example, has further cooperated with the German Federal Office for Information Security on several occasions to verify social media accounts and to institute other measures to increase cybersecurity.

A number of social media companies have announced their intention to make political ads more transparent across the **United Kingdom**. In October 2018, Facebook introduced steps aimed to prevent foreign advertising within the UK on political causes. To run politically related ads on Facebook or a linked Instagram page, the individual must prove that he or she is based in the UK using identification such as a passport, and that the advertisements will display a "paid for by" disclaimer. The "paid for by" disclaimer is a clickable link that takes users to the Ad Library, provided by Facebook, which will include information about the range of the advertisement's budget and how many people it has reached, and list any other ads that the page is running.

Social media platforms operating in **India**, including Facebook, WhatsApp, Twitter, Google, ShareChat, and TikTok, as well as the Internet and Mobile Association of India, have agreed to a Voluntary Code of Ethics for the General Election 2019. Among other measures, the platforms will provide a mechanism for notifying the Election Commission of India (ECI) of election-law violations and a method for political advertisers to submit pre-certificates issued by the ECI for running election-related ads.

Additional measures taken by social media platforms in India include the carrying by Facebook of disclaimer labels for political advertisements and the disclosure of details about those responsible for running such ads. Facebook has also been blocking fake accounts and partnering with third-party fact-checkers for the elections. Whatsapp has reportedly limited the number of times a user can forward a message to five and has labeled forwarded messages. WhatsApp has also introduced a fact-checking helpline and encouraged users to flag messages for verification.

Prior to India's recent general elections, Twitter launched a tool that allows its users to flag tweets that attempt to mislead voters.

Canada's mandatory requirement to preserve registries for political advertisements appears to have significantly impacted the way social networks handle political advertisements. Microsoft, Google, and Reddit, for example, have decided to eliminate political advertisements on their platforms before the upcoming Canadian federal election altogether in order to avoid the risk of not conforming to the law. Instead, Google announced it plans to focus on Canadian literacy programs and connecting people to relevant and useful information. Facebook, however, has decided to comply with the registry requirements, and is creating a new advertisement library that will capture details about political ads on its platform. Facebook has also started to label ads as "political" and inform readers of the person or entity paying for them. Although advertisers are expected to identify their sponsors truthfully, it has been argued that the company does not verify this information unless it is reported to be false.

According to **Israel**i media, Facebook announced that it would block anonymous, paid Israeli political ads on its site prior to the April 9, 2019, Knesset elections. Google reportedly informed Israeli media companies in early February 2019 that they would not be able to execute personal advertising on the company's systems until after the April 9 elections. This means that Google blocked all advertising options related to segmentation (advertising to a segmented audience), retargeting, and using a list of names to anyone engaged in political advertising.

Mexico's National Institute of Elections (INE) signed collaboration agreements with Facebook to train relevant INE staff and disseminate to the public informational materials to assist the public in identifying trustworthy information. INE also signed an agreement with Google to disseminate official information on the 2018 Mexican elections. Additionally, more than sixty media companies and nongovernmental organizations launched an online effort to monitor the veracity of news pertaining to the 2018 elections. Sponsors included Facebook, Google News Lab, Twitter, Open Society, and Oxfam.

A joint initiative to address fake news was created during the 2018 parliamentary election cycle in **Sweden** based on a collaboration between the two largest morning newspapers and two public service providers in that country. It evaluated the accuracy of statements by political party leaders, as well as other news stories. Other initiatives include the adoption of rules by a Swedish broadcaster allowing publication of political ads during the most recent election to the European Parliament only by Swedish political parties and Swedish unions.

Similar to the Swedish initiative to evaluate the accuracy of political statements, a **Danish** newspaper in 2017 launched a project on its website to track the content of political advertisements on Facebook related to the municipal elections by downloading all ads that users who subscribed to the service saw and thereafter sorting them as political and nonpolitical. The service reportedly provided a function whereby users could see the political advertisements that were not targeted toward them by clicking "advertisements that I cannot see."

More detailed information on the issues highlighted in this summary is provided in the individual surveys below.

Argentina

Graciela Rodriguez-Ferrand
Senior Foreign Law Specialist

SUMMARY In light of the upcoming October 2019 presidential election, the Cámara Nacional Electoral (CNE) has entered into a Digital Ethics agreement with press associations, digital platforms, and political parties to cooperate in the fight against misinformation during political campaigns and elections. A similar project has engaged media and technology companies and nongovernmental organizations to verify the truthfulness of the information available online and in social media related to the upcoming presidential election. A recent amendment to the law on financing of political parties includes specific measures aimed at enhancing the transparency and accountability of online political advertising, such as requiring those ads to be paid by credit card with full disclosure of the purchaser's identity and the registration of political parties' social media accounts.

I. Background

The widespread manipulation of fake news through social media has become a serious concern in Argentina, particularly in light of the upcoming October 2019 presidential election.[1]

Acting upon this concern, press associations, digital platforms, and political parties signed an agreement on Digital Ethics with the Cámara Nacional Electoral (CNE) (National Court on Elections) aimed at fighting misinformation during political campaigns and election periods in social networks, through cooperation with the Argentinean authorities to protect the accuracy of information within their purview.[2]

On June 11, 2019, a consortium of media and technology companies and nongovernmental organizations (NGOs), called REVERSO, began checking information related to the upcoming presidential election.[3] The consortium includes more than 100 media and technology companies jointly embarked in the fight against misinformation during the election campaign.[4] REVERSO is part of the Chequeado project, a nonpartisan and nonprofit digital media source focused on the verification of public discourse, the fight against disinformation, and the promotion of public access to information.[5]

[1] *El Impacto de las Fake News en la Campana Electoral*, Clarín (July 11, 2019), https://perma.cc/DL35-VGFY.

[2] Id.; Cámara Nacional Electoral (May 31, 2019), https://perma.cc/J9GZ-MCL6.

[3] *El Impacto de las Fake News en la Campana Electoral*, supra note 1; REVERSO, https://perma.cc/93HS-DWRJ.

[4] REVERSO, supra note 3.

[5] Chequeado, https://perma.cc/PS6S-3ZYL.

Statements of politicians, economists, businesspersons, and public figures made in social media networks are classified by the network as "true" to "false" according to their consistency with the facts and data to which they refer.[6]

II. Free Speech Protections

The right to freedom of expression is protected at the constitutional level. The Constitution proclaims that all of Argentina's inhabitants are entitled to a number of rights, in accordance with the laws that regulate their exercise, including the right to express their ideas in the press without prior censorship.[7] Additionally, Congress may not enact laws restricting the freedom of the press or establishing federal jurisdiction over it.[8]

The constitutional right to freedom of expression is not considered absolute. To meet the constitutional standard, restrictions are required to be established by law, have a legal purpose, and be proportionate to the needs of a democratic society.[9] In addition, the Supreme Court has unequivocally established that restrictions to freedom of expression must always be interpreted narrowly.[10]

There are a number of crimes related to expression in the Penal Code (CP),[11] including crimes against the public order[12] or publicly inciting collective violence against groups of persons or institutions. A person who incites such violence can be sentenced to imprisonment for three to six years.[13]

In addition, the CP provides a whole chapter on the protection of the right to honor, including penalties for slander or false accusations of crimes and the intentional dishonoring or discrediting of another person.[14]

---

[6] Id.

[7] Constitución de la Nacion Argentina, Boletín Oficial [B.O.], Jan. 3, 1995, art. 14, https://perma.cc/S3BN-9NA3.

[8] Id. art. 32.

[9] Centro de Estudios en Libertad de Expresión y Acceso a la Información, Tendencias en la Libertad de Expresión en Argentina 3 (Mar. 2018), https://perma.cc/5C6X-67WA.

[10] Id. at 4.

[11] Código Penal de la República Argentina, Ley 11.179, B.O., Nov. 3, 1921 (revised 1984), https://perma.cc/UKU8-JL7N.

[12] Id. art. 211.

[13] Id. art. 212.

[14] Id. arts. 109-117 bis.

III. Current and Pending Legislation

Law 26215 on Financing of Political Parties[15] was amended in May 2019 to include, among other changes, a provision requiring registration with the CNE of social network accounts, internet sites, and other digital communication channels of pre-candidates, candidates, and political parties and their leading officials.[16]

In each election, the legal representatives of official political parties must register the profiles of pre-candidates and candidates.[17]

At the time they report their digital platform campaign expenses, political parties are required to submit all audiovisual material pertaining to the political campaign that is available on the internet, social media networks, messaging, and any other digital platform.[18]

IV. Other Government Actions

Thirty days before an election, the CNE will offer institutional messages of civil and digital education in digital environments, in order to raise awareness of the responsible and critical use of election information available on the internet.[19]

The CNE issued technical recommendations through its accounting auditors to implement the legal changes enacted by the recent amendments to Law 26215.[20] The guidelines indicate that political parties must pay online political advertising only by credit card with full disclosure of the identity of the person or entity purchasing such ads.[21]

V. Media Coordination

In April 2019, Facebook and the CNE signed a memorandum of cooperation (MOC), under which Facebook will monitor suspicious or illegal activity during the upcoming presidential election season.[22] Facebook will make a redirect button to the CNE website available on its platform to users in Argentina, where voters can find their voting locations and hours, identification

[15] Ley 26215 de Financiamiento de los Partidos Políticos, B.O., Jan. 17, 2007, https://perma.cc/AKF5-NRDY, as amended by Ley 27504, B.O., May 31, 2019, https://perma.cc/LFX2-9433.

[16] Ley 27504, art. 19.

[17] Id. art. 43 decies.

[18] Id. art. 43 undecies.

[19] Id. art. 43 duodecies.

[20] Cuerpo de Auditores Contadores, CNE, Anexo I, Recomendaciones Técnicas del Cuerpo de Auditores Contadores a las Agrupaciones Políticas sobre Informes de Campana Electoral y los Balances Anuales Conforme a los Cambios Introducidos por la Ley 27.504 modificatoria de la Ley 26215 y Nueva Jurisprudencia, https://perma.cc/K2C5-NQX7.

[21] Id. at 3.

[22] Memorandum of Cooperation CNE–Facebook, Buenos Aires (Apr. 19, 2019), https://perma.cc/7FBX-KKE9.

documents required in order to vote, how to contact the electoral authority, and other relevant information.[23]

Under the MOC, external websites linked to a redirect button on Facebook's platform have to be vetted beforehand by Facebook. The CNE and Facebook will jointly consider carrying out events aimed at informing the public about the election and the role of Facebook as a platform for civic engagement.[24]

[23] Id.

[24] Id.

Australia

Kelly Buchanan
Foreign Law Specialist

SUMMARY The Australian government and Parliament have taken several actions in the past two years with respect to protecting democratic systems from interference, including cyberattacks and the distribution of disinformation via the internet. Legislative actions have included enhancing the requirements for authorization statements for campaign advertising under the electoral law, with the requirements specifically extended to social media pages and posts. New criminal offenses have been introduced that target acts of foreign interference that influence a political or government process, impact the exercise of a democratic political right or duty, or prejudice national security. In addition, a new foreign influence transparency register has been established and those who undertake communications activity in Australia on behalf of the foreign principal for the purpose of political or governmental influence must make disclosure statements, including on social media posts.

Legislation passed in April 2019, following the mosque attacks in Christchurch, New Zealand, requires social media companies to remove abhorrent violent material in an expeditious manner. The relevant offenses in the law apply to both individuals and companies responsible for hosting online content.

In 2018, the Australian government established the Electoral Integrity Assurance Taskforce, made up of representatives from several government agencies. The task force seeks to protect Australia's democracy against malicious cyberactivity, physical means, electoral fraud, foreign interference, and disinformation. The parliamentary committee on electoral matters also recommended that its successor committee in the new parliamentary session, commencing following the May 2019 federal election, address the negative impact of disinformation on democracy as an ongoing inquiry.

In the lead-up to the May 2019 federal election, the Australian Electoral Commission (AEC) launched the "Stop and Consider" campaign, aimed at encouraging voters to consider the source of any electoral communication. During 2018, when several by-elections were held, and prior to the 2019 election, the AEC also engaged with social media companies with respect to ensuring compliance with electoral law, particularly the requirements for authorization statements on electoral communications. This included sending a document to Facebook and Twitter setting out its expectation that these companies will "respond to its notifications of illegal ads by either removing or blocking the post, or by passing on the details of the creator of the ad to the AEC." According to the AEC, both companies had broadly complied with the procedures in the document.

Prior to the federal election, Twitter and Facebook also released policies regarding Australian political advertising on the two social media platforms. Facebook stated that it would ban electoral ads purchased from outside Australia, starting the day after the announcement of the federal election. It also partnered with a fact-checking provider, with stories rated false being lowered in the News Feed. Twitter required political

campaigning advertisers to apply for certification from the company, meet certain profile requirements, and comply with applicable Australian laws. It also prohibited the purchasing of advertising using foreign payment methods.

During the 2019 election campaign, the Labor Party engaged with Facebook over the appearance of false stories on the platform regarding a purported "death tax" policy. Following the election, the party sought a formal report from the company regarding the steps it had taken to combat the spread of this misinformation campaign.

I. Background

The spread of disinformation using the internet, and social media platforms in particular, is recognized as a serious concern in Australia. A global survey completed in early 2018 showed that trust in the media in the country "is at a record low of just 31% and consumers say they struggle to tell the difference between fake news and facts."[1] During the lead up to the recent federal election, held in May 2019, one political party asked Facebook to remove posts containing false information about plans to introduce a "death tax," the Australian Electoral Commission (AEC) worked with Facebook and Twitter to establish processes for the removal of content that violated election laws, Facebook announced it would prohibit foreign political advertising targeting Australians, Twitter implemented new rules related to labeling and proof of location, and the AEC launched a campaign to encourage voters to consider the source of online information.[2]

Previously, in 2018, the government established a task force aimed at protecting elections from foreign interference and cyberattacks. Legislation also came into force that enhances the requirements in the Commonwealth Electoral Act 1918 (Cth)[3] and other laws with respect to authorization statements on campaign advertisements, including extending the requirements to social media posts. Other legislative actions with potential impacts on social media companies and users included the introduction of new secrecy and foreign interference offenses, and disclosure requirements for communications on behalf of foreign principals. Recently, in April 2019, legislation was enacted requiring social media companies to remove violent material.

Parliamentary select committees have considered issues related to disinformation in the context of inquiries into the conduct of the 2016 Australian federal election[4] and the future of public interest journalism,[5] with references made to the issues that emerged in the 2016 US federal

[1] Amanda Meade, *Australia's Trust in Media at Record Low as 'Fake News' Fears Grow, Study Finds*, The Guardian (Feb. 6, 2018), https://perma.cc/9G6K-5KYX.

[2] See Michael Jensen, *Fake News is Already Spreading Online in the Election Campaign – It's Up to Us to Stop It*, The Conversation (Apr. 23, 2019), https://perma.cc/T9BA-7F7W.

[3] Commonwealth Electoral Act 1918 (Cth), https://perma.cc/93K5-6P8V.

[4] Joint Standing Committee on Electoral Matters (JSCEM), *Report on the Conduct of the 2016 Federal Election and Matters Related Thereto* (Nov. 2018), https://perma.cc/2NDM-DLQG.

[5] Senate Select Committee on the Future of Public Interest Journalism, *Report* (Feb. 2018), https://perma.cc/9M9Q-GW5R.

elections and UK Brexit referendum campaign. In addition, in 2018, the Australian Competition and Consumer Commission released a preliminary report on its inquiry into digital platforms in which it made recommendations related to addressing the market power of certain internet companies and monitoring digital platforms' activities.[6] Most recently, in its March 2019 status report, published prior to the federal election, the Joint Standing Committee on Electoral Matters (JSCEM) stated that "[t]he negative impact of disinformation on democracy is now a global concern. . . . the Committee would like to see its successor addressing this threat as an ongoing inquiry. This would include engaging with international counterparts to form global solutions to a global problem."[7] It dedicated a chapter in its report to discussing this issue and possible solutions, both at the global and domestic level.

Australia does not have a federal bill of rights and its Constitution does not explicitly protect freedom of speech, expression, or the media.[8] However, the High Court of Australia has recognized an implied right to freedom of political expression in the Constitution. The JSCEM discussed this right, and possible restrictions on it, in a chapter on democracy and digital technology contained in its report on the conduct of the 2016 federal election. The report notes that, based on High Court decisions, "Parliament can, in some instances, impose restrictions; balancing the need for such measures with the importance of political discussion."[9] It cites the case of *Lange v Australian Broadcasting Corporation*, which set out a two-step test for the validity of any restrictions on the right in legislation:

> First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end the fulfilment of which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government and the procedure prescribed by s 128 for submitting a proposed amendment of the Constitution to the informed decision of the people . . . If the first question is answered 'yes' and the second is answered 'no', the law is invalid.[10]

The report notes that a further restriction was included in the High Court's decision in *Australian Capital Television Pty Ltd v Commonwealth*:

> [H]aving regard to the conceptions of representative government, Parliament has no right to prefer one form of lawful electoral communication over another. It is for the electors and the candidates to choose which forms of otherwise lawful communication they prefer to

[6] Australian Competition & Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (Dec. 2018), https://perma.cc/JSE2-V2DR.

[7] JSCEM, *Status Report* 1-2 (Mar. 2019), https://perma.cc/JST3-W38F.

[8] See *Freedom of Information, Opinion and Expression*, Australian Human Rights Commission (May 1, 2013), https://perma.cc/9HK9-LPLE.

[9] JSCEM, *Report on the Conduct of the 2016 Federal Election and Matters Related Thereto*, supra note 4, at 167.

[10] Id. (quoting *Lange v Australian Broadcasting Corporation* [1997] HCA 25, https://perma.cc/B6KD-WTF2).

> use to disseminate political information, ideas and argument. Their choices are a matter of private, not public, interest. Their choices are outside the zone of governmental control.[11]

The JSCEM concluded that "[t]his must be remembered when attempting to address online political communication and contrasting it to more 'traditional' advertising. However, it is not an insurmountable obstacle to redressing dark advertising or disinformation."[12]

In addition to the above considerations, part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011 (Cth) requires that the government assess bills for their compatibility with the human rights and freedoms recognized or declared in certain international instruments.[13] Compatibility statements must accompany bills and disallowable legislative instruments.[14]

II. Current and Pending Legislation

In an article published in May 2019, just prior to the federal election, an academic at the University of Melbourne stated that there seems to be little understanding across the political spectrum in Australia when it comes to

- the regulation of social media platforms
- the rise and spread of fake news
- the abuse and security of user data
- the fomentation of hate speech [and]
- how cyberbullying and harassment play out in the real world, and their impact[.][15]

She argued that "the major parties, with the exception of The Greens who are calling for an inquiry and regulation of social media, have failed to make policy connections to better online governance, whether in relation to data handling or content regulation."[16]

Following the federal election, an article published in *The Guardian* discussed various false claims made during the election and their propagation by fringe groups on social media. It said that this year's campaign has led to calls for reforms targeting misleading and deceptive political advertising from several members of Parliament.[17] According to the article, however, "[r]eform has routinely been described as unworkable and a potential restriction of free speech. Previous

---

[11] Id. (quoting *Australian Capital Television Pty Ltd v Commonwealth* [1992] HCA 45, https://perma.cc/2LDL-Z2MY).

[12] Id. at 168.

[13] Human Rights (Parliamentary Scrutiny) Act 2011 (Cth) pt 3, https://perma.cc/K4YH-UZB4.

[14] See *Statements of Compatibility*, Attorney-General's Department, https://perma.cc/YWT7-8MLC.

[15] Jennifer Beckett, *Major Parties Staying Silent on Social Media Regulation*, Election Watch, University of Melbourne (May 13, 2019), https://perma.cc/4A3T-S26R.

[16] Id.

[17] Christopher Knaus & Nick Evershed, *False Election Claims Spark Push for Truth in Political Advertising Laws*, The Guardian (May 20, 2019), https://perma.cc/HYK6-DGY6.

attempts to regulate advertising have failed dramatically. In the 1980s, parliament attempted to introduce such laws before quickly repealing them."[18]

In the past two years, legislative reforms that potentially impact social media platforms and users have sought to enhance transparency in political advertising, introduced new offenses related to foreign interference and sharing information that affects national security, established a registration system and disclosure requirements where communications are made on behalf of a foreign principal, and imposed a new requirement on internet companies to remove "abhorrent violent material."

A. Electoral and Other Legislation Amendment Act 2017

The Australian government introduced the Electoral and Other Legislation Amendment Bill 2017 in March 2017 in response to the JSCEM's interim report on the 2016 federal election that focused on authorization requirements for voter communication.[19] The bill was passed in September 2017 and the amendments came into force in March 2018, prior to several federal by-elections held during 2018.[20] In summary, the bill

- applies the electoral authorisation requirements to modern communication channels
- requires all paid electoral advertising (which includes distribution or production) to be authorised, no matter the source
- makes the information provided in authorisations more useful to voters by requiring those subject to the Commonwealth electoral funding and finance disclosure regime (disclosure entities) to include this information in their political communications
- ensures the obligation to authorise electoral and referendum matter primarily rests with those responsible for the decision to communicate it
- replaces the current criminal non-compliance regime with a civil penalty regime to be administered by the Australian Electoral Commission [and]
- harmonises authorisation requirements across broadcasting, electoral, and referendum legislation, while retaining current requirements in relation to specified printed materials[.][21]

The authorization requirements for political advertising in Australia are contained in part XXA of the Commonwealth Electoral Act 1918 (Cth) and the Commonwealth Electoral (Authorisation

[18] Id.

[19] *Electoral and Other Legislation Amendment Bill 2017*, Parliament of Australia, https://perma.cc/G753-75PB; JSCEM, *The 2016 Federal Election: Interim Report on the Authorisation of Voter Communication* (Dec. 2016), https://perma.cc/5YYL-A8LW. See also Damon Muller, *Electoral and Other Legislation Amendment Bill 2017* (Bills Digest No. 10, 2016-17, May 26, 2017), https://perma.cc/HR99-V7C7.

[20] Electoral and Other Legislation Amendment Act 2017 (Cth) s 2, https://perma.cc/5H22-AE4P; Press Release, Australian Electoral Commission (AEC), New Rules for Authorising Electoral, Referendum and Political Matter (Mar. 6, 2018), https://perma.cc/3D5W-FXPG.

[21] Parliament of Australia, Senate, *Electoral and Other Legislation Amendment Bill 2017: Revised Explanatory Memorandum* 2, https://perma.cc/RA6T-AGXC.

of Voter Communication) Determination 2018 (Cth),[22] in schedule 2 of the Broadcasting Service Act 1992 (Cth),[23] and in part IX of the Referendum (Machinery Provisions) Act 1984 (Cth).[24] The AEC has produced a document that explains the requirements in detail, including those that apply to social media communications.[25] In a blog post, the Australian Parliamentary Library provides a brief outline of the requirements:

> Whereas in previous elections the law was somewhat unclear as to the extent that social media posts required authorisation, having been written long before social media existed, the new laws explicitly include social media posts, bulk text messages, and recorded phone messages (robocalls).
>
> The rules also have a number of specific requirements for authorisation of different types of communication. Social media posts, for example, must have the required details at the end of the message, or if there is insufficient room, in an image in the post or at a website accessed through a URL in the post (authorisation details in a Facebook or Twitter bio will also generally be sufficient, according to the AEC). Phone calls (and robocalls) must have the details at the start of the message, and streamed music (such as Spotify ads) at the end of the music.[26]

The post also explains that,

> [g]enerally, electoral communication only requires authorisation if it has been paid for (such as a promoted tweet, a search advertisement, or a TV ad), if it is a promotional item (such as a flyer, sticker, poster or how-to-vote card), or if it is communicated by or on behalf of a disclosure entity and is intended to affect voting in a federal election.
>
> Candidates, parties and their associated entities are all disclosure entities, as are political campaigners and third parties (organisations or people who have incurred significant electoral expenditure). In addition, people or organisations who have donated more than the disclosure threshold (currently [AU]$13,800 [about US$9,625]) to a political party, political campaigner or third party are also disclosure entities, and their electoral communication will need to carry the required particulars.[27]

The Commonwealth Electoral Act 1918 (Cth) contains a table setting out the authorization particulars,[28] which must include

---

[22] Commonwealth Electoral (Authorisation of Voter Communication) Determination 2018 (Cth), https://perma.cc/TD6V-64NW.

[23] Broadcasting Services Act 1992 (Cth) sch 2, https://perma.cc/K8YK-YYVH.

[24] Referendum (Machinery Provisions) Act 1984 (Cth) pt IX, https://perma.cc/SUX6-QCJY.

[25] *Electoral Backgrounder: Electoral Communications and Authorisation Requirements*, AEC (updated July 16, 2019), https://perma.cc/9UEP-HL5T.

[26] Damon Muller, *Online Political Communication – Does This Post Need to be Authorised?*, FlagPost (Apr. 23, 2019), https://perma.cc/5EFM-XUVK.

[27] Id.

[28] Commonwealth Electoral Act 1918 (Cth) s 321D(5).

- where the person who authorised the communication is an individual, the name of the person and the relevant town or city of the person;
- where the communication is authorised by a disclosure entity (e.g. a registered political party) the name of the entity, the relevant town or city of the entity and the name of the natural person within the disclosure entity responsible for giving effect to the authorisation; [and]
- where the communication is authorised by an entity that is not a disclosure entity or a natural person (e.g. a company that is not an associated entity) the name of the entity and the town or city of the entity.[29]

The requirement for the placement of authorization particulars on social media posts are contained in the 2018 Determination.[30]

B. National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018

In June 2018, the Parliament passed a bill containing various national security legislation amendments.[31] This included the addition of new secrecy provisions to the Criminal Code Act 1995 (Cth). Among these provisions, for example, is a new offense of communicating information obtained from a federal official, where that information has a high-level security classification or where its communication "damages the security or defence of Australia," interferes with or prejudices law enforcement activities, or "harms or prejudices the health and safety of the Australian public or a section of the Australian public."[32] There are several defenses available to such offenses, including where the person communicated the relevant information in his or her capacity as "a person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in the news media" and he or she believed that engaging in the conduct was in the public interest.[33]

The 2018 amendments also added new foreign interference offenses to the Criminal Code. These include where a person engages in conduct on behalf of, in collaboration with, or that is directed or funded by a foreign principal with the intent of influencing a political or government process, the exercise of an Australian democratic political right or duty, or prejudicing Australia's national security, and any part of that conduct is covert or involves deception.[34] A similar offense applies where the person was reckless as to the influence of his or conduct on political or governmental processes, democratic rights, or national security.[35]

[29] *Electoral Backgrounder: Electoral Communications and Authorisation Requirements*, supra note 25.

[30] Commonwealth Electoral (Authorisation of Voter Communication) Determination 2018 (Cth) cl 9(1), item 4.

[31] National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Cth), https://perma.cc/8GAE-LXUR.

[32] Criminal Code Act 1995 (Cth) s 122.4A(1), https://perma.cc/NQM8-W3X5.

[33] Id. s 122.5(6).

[34] Id. s 92.2(1).

[35] Id. s 92.3(1).

C. Foreign Influence Transparency Scheme Act 2018

The Foreign Influence Transparency Scheme Act 2018 (Cth),[36] also passed in June 2018, established a new system that

> introduces registration obligations for persons and entities who have arrangements with, and undertake certain activities on behalf of, foreign principals. Whether a person or entity is required to register will depend on who the foreign principal is, the nature of the activities undertaken, the purpose for which the activities are undertaken, and in some cases, whether the person has held a senior public position in Australia.[37]

In addition, under the Scheme, certain disclosure requirements are imposed on people and entities who

- undertake communications activity in Australia on behalf of the foreign principal for the purpose of political or governmental influence, or
- produce information or material on behalf of a foreign principal for the purpose of being communicated or distributed to the public[.][38]

These concepts "relate to the production or communication/distribution of information in any material or any form," including electronic messaging and communication via social media.[39] The disclosure requirements apply even if a person has not yet registered under the Scheme. The Attorney-General's Department explains that

> [a] person undertaking communications activity must ensure they make a disclosure about the fact that the information or material is produced, communicated or disseminated on behalf of a foreign principal and is a registrable activity under the Foreign Influence Transparency Scheme Act 2018 (the Act).
>
> The details of the disclosure requirements for different types of communications activities, including where and when the disclosure should occur, and in what form, are prescribed by the Foreign Influence Transparency Scheme (Disclosure in Communications Activity) Rules 2018. These details depend on the type of communication activity being undertaken, such as whether it is printed or audio communications. However, the substance of the disclosure is the same regardless of the type of communications activity.
>
> The disclosure must:
> - identify who is undertaking the communications activity (usually the person who is required to be registered under the scheme)
> - identify the foreign principal on whose behalf the communications activity is undertaken (for example, the relevant foreign government, entity or person)

[36] Foreign Influence Transparency Scheme Act 2018 (Cth), https://perma.cc/2FZD-2DP5.

[37] *Foreign Influence Transparency Scheme*, Attorney-General's Department, https://perma.cc/R5R9-4CB7.

[38] Attorney-General's Department, *Foreign Influence Transparency Scheme: Factsheet 10 – Disclosures in Communications Activity* 1 (Apr. 2019), https://perma.cc/D5P2-4ZSR.

[39] Id.

- state that the communications activity is undertaken on behalf of the foreign principal, and
- state that the disclosure is made under the Act.[40]

The disclosure rules include specific requirements with respect to the placement of the relevant disclosure statement for communication activity involving communication or distribution by social media.[41]

D. Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019

In April 2019, following the March 2019 mosque attacks in Christchurch, New Zealand, the Australian Parliament passed legislation[42] establishing new offenses in the Criminal Code that require providers of internet, hosting, or content services (including social media platforms) to ensure the "expeditious removal" of "abhorrent violent material" that can be accessed in Australia,[43] and to refer details of such material that has occurred in Australia to the Australian Federal Police.[44] "Abhorrent violent material" is defined as material that records or streams abhorrent violent conduct and is material that "reasonable persons would regard as being, in all the circumstances, offensive."[45] It also needs to be produced by a person who engaged in the violent conduct, or who "aided, abetted, counselled or procured, or was in any way knowingly concerned in, the abhorrent violent conduct."[46] "Abhorrent violent conduct" is defined as including terrorist acts, murder and attempted murder, torture, rape, and kidnapping.[47]

An offense of failing to remove abhorrent violent material is punishable by imprisonment of up to three years or a fine of up to AU$2.1 million (about US$1.47 million) for an individual, or a fine of up to AU$10.5 million (about US$7.32 million) or 10% of annual turnover, whichever is greater, if the offender is a company.[48]

The subdivision in the Criminal Code containing the relevant offenses does not apply "to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication."[49] In addition, defenses in the legislation include where the material relates to a

[40] Id. at 2.

[41] Foreign Influence Transparency Scheme (Disclosure in Communications Activity) Rules 2018 (Cth) r 5 item 6, https://perma.cc/KY3V-ZNTT.

[42] *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019*, Parliament of Australia, https://perma.cc/UV8K-FHDJ; Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Cth), https://perma.cc/PC8U-CGE9.

[43] Criminal Code Act 1995 (Cth) s 474.34.

[44] Id. s 474.33.

[45] Id. s 474.31(1)(a) & (b).

[46] Id. s 474.31(1)(c).

[47] Id. s 474.32.

[48] Id. s 474.34(9) & (10).

[49] Id. s 474.38(1).

news or current affairs report that is in the public interest,[50] and another defense is that the accessibility of the material is for the purpose of "advocating the lawful procurement of change to any matter established by law, policy or practice" in Australia or a foreign country.[51]

Legal experts, the technology sector, and media companies criticized the legislation, arguing it was drawn up and passed too hastily, without consultation, and does not address hate speech, and that the vast volumes of content uploaded to the internet makes the problem highly complex.[52]

III. Other Government Actions

A. Electoral Integrity Assurance Taskforce

In June 2018, news outlets reported that the Australian government had established the Electoral Integrity Assurance Taskforce "to guard against cyberattacks and interference in elections."[53] The task force is led by the Department of Home Affairs, with involvement from the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP).[54] The AEC's website states that

> [t]hreats to our democracy through malicious cyber activity, physical means, electoral fraud, foreign interference or disinformation are a matter of concern for every Australian.
>
> The Electoral Integrity Assurance Taskforce (Taskforce), made up of representatives from a range Commonwealth government agencies is working together to protect our electoral integrity.[55]

Ahead of the 2019 federal election, Australian Electoral Commissioner Tom Rogers stated that the AEC had "worked with our security partners including the Australian Signals Directorate, the Australian Cyber Security Centre and others to examine our own systems and also to examine the processes we put around our systems to defend them," according to *The Sydney Morning Herald*:

> There has been heightened international concern about foreign interference in elections especially after American intelligence officials revealed the Russian government attempted to influence the 2016 US presidential vote.

---

[50] Id. s 474.37(1)(e).

[51] Id. s 474.37(1)(h).

[52] See Paul Karp, *Australia Passes Social Media Law Penalising Platforms for Violent Content*, The Guardian (Apr. 4, 2019), https://perma.cc/6VPM-Q9EM; Rohan Pearce, *FAQ: Australia's New 'Abhorrent Violent Material' Laws*, Computerworld (Apr. 4, 2019), https://perma.cc/72MU-BNA5.

[53] Will Ziebell, *Australia Forms Task Force to Guard Elections from Cyber Attacks*, Reuters (June 9, 2018), https://perma.cc/2YEL-JWNH.

[54] *Anti-Meddling Task Force Set Up Ahead of Australian By-Elections*, SBS News (June 6, 2018), https://perma.cc/H4AF-PYBJ.

[55] *Electoral Integrity: 2019 Federal Election*, AEC (updated Apr. 12, 2019), https://perma.cc/AMT3-23DL.

> Mr Rogers said there is "no evidence of any compromise of the electoral systems owned by the AEC."
>
> There is also no evidence that foreign state-backed actors have attempted to hack the commission's systems ahead of the May federal election.
>
> "We are liaising at the moment almost daily with relevant security agencies about those sorts of issues and they help us monitor our own systems so I'm pretty comfortable with where we are with that," Mr Rogers said.
>
> . . .
>
> Mr Rogers said the commission is "monitoring what is going on internationally" with interference in elections and is in regular contact with election management agencies in countries including Canada, UK, New Zealand and the US. But he warned that every electoral system is at some risk.[56]

In its report on the 2016 election and subsequent status report, the JSCEM had recommended the establishment of a permanent task force to "prevent and combat cyber-manipulation in Australia's democratic process."[57] It also recommended that the task force consider "clarification of the legal framework surrounding social media services and their status as a platform or publisher";[58] however, this aspect does not appear to be included in the Electoral Integrity Assurance Taskforce's mandate.

B. "Stop and Consider" Campaign

Prior to the 2019 federal election, the AEC launched a social media advertising campaign to encourage voters to "carefully check the source of electoral communication they see or hear."[59] The initiative, called "Stop and Consider," involved advertising on platforms such as Facebook, Twitter, and Instagram,[60] as well as an AEC webpage.[61] The AEC noted that,

> [u]nder the Commonwealth Electoral Act 1918, there are no provisions relating to truth in electoral communication in respect of political claims and counter claims, and the AEC has no legislative power in this area. Australian voters have the freedom and right to express a political opinion or critique an election policy, either in-person or via social media.[62]

---

[56] Matt Wade, *AEC in Constant Contact with Security Agencies to Protect Federal Election*, The Sydney Morning Herald (Mar. 1, 2019), https://perma.cc/XEE4-PNZW.

[57] JSCEM, *Status Report*, supra note 7, at 8.

[58] Id.

[59] Press Release, AEC, AEC Encouraging Voters to "Stop and Consider" This Federal Election (Apr. 15, 2019), https://perma.cc/939W-8DQS.

[60] Id.

[61] *Stop and Consider: Check the Source This Federal Election*, AEC (updated Apr. 12, 2019), https://perma.cc/A9X8-93ED.

[62] Press Release, AEC, supra note 59.

While it has no role checking the truth of electoral communications, the AEC does provide a complaint form for members of the public to submit information about communications that have not been correctly authorized.[63] An AEC spokesperson said that "[t]he nature of advertising on social media means that the AEC depends on tip-offs or complaints about the authorisation of electoral advertising on social media."[64]

IV. Media Coordination

A. AEC Engagement with Facebook and Twitter in 2018

In February 2019, an investigation by the Australian Broadcasting Corporation (ABC) using documents obtained under freedom of information laws showed that the AEC had contacted Facebook in 2018 after it became concerned about a particular group paying for sponsored posts attacking left-wing groups and political parties in Australia. Due to the lack of correct authorization information on the advertising, the AEC asked Facebook to provide the identity of those responsible for the relevant page, or to otherwise block or remove the page until it complied with the requirements in the Commonwealth Electoral Act 1918 (Cth). The ABC reported that

> Facebook initially appeared willing to help the AEC make sure those ads carried the required authorisation, but did not provide the AEC with any information about who was behind the page.
>
> "I passed this along to our govt case work team as an urgent escalation to see what can be done about this page, including whether it can be geoblocked until an authorisation is included," Ms Malloch [of Facebook] wrote in her reply to Mr Johnson [of the AEC].
>
> But five days later, Ms Malloch sent a follow-up email, brushing aside the AEC's concerns.
>
> "The Hands Off Democracy page appears to contain organic user content, rather than advertising paid for through Facebook's online advertising process, and does not seem to require authorisation," she wrote.
>
> "If you have a different view please let me know."
>
> Mr Johnson responded by sending a screenshot of a sponsored post by Hands Off Our Democracy, which attacked The Greens and the activist group GetUp! and did not include the correct authorisation.
>
> Mr Johnson said the screenshot indicated the group's page "has (or did have) sponsored content".
>
> A series of email exchanges between Mr Johnson and Ms Malloch followed, in which the pair discussed whether the page should carry authorisation information.

[63] *Stop and Consider*, supra note 61; *I'd Like to Make a Complaint*, AEC, https://perma.cc/4NL7-SPDT.

[64] Lucy Battersby, *Voters Asked to Dob in Illegal Political Ads Appearing on Social Media*, The Sydney Morning Herald (Feb. 18, 2019), https://perma.cc/J53W-H32F.

> But before the AEC's concerns were addressed, Hands Off Our Democracy's page disappeared from Facebook.
>
> Finally, on August 14 — more than a month after the matter was raised with Facebook — Ms Malloch conceded that the page was indeed paying for ads.
>
> "It appears that this page was removed by the administrator before we could take any action, but yes you are correct — the 'sponsored' posts were ads," she wrote.
>
> Facebook said the reason it did not take further steps is because when it reviewed the page on July 4, it no longer contained paid ads.
>
> Therefore, it did not appear to be in breach of any electoral rules.
>
> "We have a productive relationship with the Australian Electoral Commission and have an established dedicated escalation path for the AEC to notify us of any advertising content that violates the Electoral Act," Facebook said in a statement to the ABC.
>
> "When this happens, we will block the content out of respect for local law."
>
> The sponsored post attacking Get Up! and The Greens had received hundreds of likes and comments and had been shared widely prior to its disappearance from Facebook.[65]

Following the discussion regarding the particular ads, the AEC "sought to create a formal set of protocols for social media companies to deal with potentially illegal political ads."[66] The relevant document, sent to Facebook and Twitter, made it clear that the AEC expects these companies to "respond to its notifications of illegal ads by either removing or blocking the post, or by passing on the details of the creator of the ad to the AEC."[67] The AEC said it may go to court to seek an injunction against the relevant company or the responsible user in the event of noncompliance. In a statement to the ABC, the AEC said that both Twitter and Facebook "have been broadly complying with the document they received last year."[68]

B. Meetings with Internet Companies

In February 2019, the AEC stated that it had "productive meetings" with Facebook, Twitter, and Google during the electoral cycle, including discussions about the new authorization requirements.[69] It was also reported that ASIO had met with Facebook and Google to discuss how to address foreign interference and disinformation during the federal election campaign.[70]

---

[65] Pat McGrath, *Facebook Probed by Australian Electoral Commission over Mysterious Political Ads*, ABC News (Feb. 25, 2019), https://perma.cc/KKW3-SZFA.

[66] Id.

[67] Id.

[68] Id.

[69] Ariel Bogle, *Twitter Rolls Out New Advertising Rules to Fight Political Misinformation*, ABC News (Feb. 19, 2019), https://perma.cc/863C-22DP.

[70] Lanai Scarr, *ASIO Meets with Facebook and Google over Upcoming Election*, The West Australian (Feb. 14, 2019), https://perma.cc/FYH4-YU35.

Australia's prime minister and attorney-general met with social media companies in response to the March 2019 Christchurch mosque attacks, prior to the passage of the legislation aimed at violent material, discussed above.[71]

C. Facebook's Policy on Australian Political Advertising

In early April 2019, Facebook said that it would "ban political advertising bought by foreign entities and crack down on fake accounts during the federal election."[72] The company's director of policy in Australia, Mia Garlick, indicated the company would take a "multi-pronged approach."[73] In a blog post, she stated that the temporary ban on electoral ads purchased from outside Australia, starting the day after the announcement of the federal election, "will apply to ads we determine to be coming from foreign entities that are of an electoral nature, meaning they contain references to politicians, parties or election suppression. We also won't allow foreign ads that include political slogans and party logos."[74] In addition, she stated that Facebook had partnered with the news wire service Agence France-Presse in order to conduct third-party fact checking in Australia. This could lead to a story being rated as false, which then lowers it in the News Feed, "reducing its future views by more than 80% on average."[75]

Other actions referred to in the blog post included the "Ad Library," which aims to make Facebook ads more transparent; removal of content that violates its Community Standards; blocking of fake accounts; employing more people to work on safety and security across the platform; and improving its machine learning capabilities around political content and inauthentic behavior.[76]

D. Twitter's Policy on Australian Political Advertising

In February 2019, Twitter announced new rules related to political advertising on the platform in order to comply with the authorization requirements in Australia's electoral laws.[77] Its policy statement, which applies to federal elections only, reads as follows:

---

[71] Paul Osborne, *Scott Morrison Vows Crackdown on Social Media Giants, Threatening Jail Terms and Multimillion-Dollar Fines*, News.com.au (Mar. 30, 2019), https://perma.cc/Y3EU-2ALL.

[72] Jessica Rowe, *Facebook Bans Foreign Political Ads in Lead Up to Australian Election*, SBS News (Apr. 5, 2019), https://perma.cc/XXK5-C5UD; Tom Westbrook, *Facebook Promises Crackdown on Fake News in Australia*, Reuters (Apr. 4, 2019), https://perma.cc/J2VV-CJ4W; Jennifer Duke, *Facebook to Block Foreign Ads, Start Fact-Checking Ahead of Election*, The Sydney Morning Herald (Apr. 5, 2019), https://perma.cc/T82J-8RWC.

[73] Rowe, supra note 72.

[74] Mia Garlick, *Working to Safeguard Elections in Australia*, Facebook Newsroom (Apr. 4, 2019), https://perma.cc/4NJR-QC5T.

[75] Id.

[76] Id.

[77] Bogle, supra note 69.

Political Content includes political campaigning and issue advocacy advertising.

- Political campaigning ads are permitted but must meet additional eligibility requirements and apply for certification.
- Issue advocacy ads are permitted without restriction.

Political campaigning ads may only be promoted via the use of Promoted Tweets and In-Stream Video Ads; no other Twitter advertising products can be used at this time.

Political Campaigning

Policy
Political campaigning ads refers to ads that fall under any of the criteria listed below:

- Ads purchased by a political party, candidate, or entity registered with the Australian Election Commission; or
- Ads that advocate for or against a clearly identified candidate or party for Australian federal elections.

Requirements
Political campaigning advertisers must go through Twitter's certification process and meet the following requirements:

- Profile photo, header photo, and website must be consistent with the handle's online presence.
- Bio must include a website that provides valid contact info.
- If handle name is not related to the certified entity, the bio must include the following disclaimer: "Owned by [certified entity name]".

Restrictions
- Political campaigning advertisers must comply with applicable Australian laws regarding disclosure and content requirements, eligibility restrictions, spending limits, reporting requirements, and blackout dates.
- Political campaigning advertisers are prohibited from using foreign payment methods.

Once certified, political campaigning advertisers will be prompted to use "Paid for by" and "Authorized /not authorized" disclaimers. Disclaimers must not be misleading and match website or certification application.[78]

The certification process is listed on a separate page that covers several countries. Applicants are required to have an advertiser account and must submit an application. The information required for entities that wish to advertise in Australia are as follows:

[78] *Political Content in Australia*, Twitter, https://perma.cc/HJ85-4J3N.

- **Political parties, candidates, or entities registered with the AEC**
  - Name and address as it appears in the AEC registry.

- **Organizations not registered with the AEC**
  - Australia Business Number (ABN)

- **Individuals**
  - Government-issued photo ID
  - Utility bill not older than 3 months if the government-issued ID does not contain an address or the person is unable to receive physical mail in such address.[79]

Twitter has also published frequently asked questions related to its political campaigning policy with respect to Australia, EU parliamentary elections, India, and the United States.[80]

E. Misinformation During 2019 Election Campaign

In April 2019, the Labor Party "demanded Facebook investigate apparent 'fake news' posts claiming the opposition is planning to introduce a 'death tax' on inheritances, in the first major test of the social media giant's promise to crack down on false election material."[81] Following the election, *The Guardian* conducted an investigation into the course and impact of the "death tax" claims. According to the report, published in early June 2019, as the election neared,

> Labor again contacted Facebook to request urgent intervention. A fresh dossier of material was handed to the social media giant on the weekend of 11-12 May. There were high level contacts between [Labor's national secretary, Noah] Carroll and senior Facebook executives, but also staff-to-staff interactions. Facebook staff said they did not believe the sharing was the result of an organised campaign driven by bots that would indicate the possibility of foreign interference.
>
> On 14 May, five days out from election day, Carroll and other Labor campaign staff had a second phone hook-up with Garlick and her team. Carroll later told colleagues he did not mince words, declaring the platform was disseminating flat-out lies, not the exaggerations of daily politics, and Facebook was accepting advertising money from politicians promoting lies.
>
> The Labor operatives did not allege foreign interference, but compared the misinformation to episodes in the American presidential campaign of 2016, and during the Brexit referendum campaign in the UK. "We stressed from our perspective, this could not be any more serious," one insider says.
>
> Facebook responded by advising it had looked at the supplied material and referred it for third-party fact-checking. Some of the material had been found to be false and would be subject to demotion in the Newsfeed. Carroll sought clarification about what that meant. Facebook advised this meant the material would be less prominent.

[79] *How to Get Certified as a Political Campaigning Advertiser*, Twitter, https://perma.cc/47PS-M56C.

[80] *Political Campaigning Policy FAQs*, Twitter, https://perma.cc/L3PV-8ULA.

[81] David Wroe, *Labor Demands Facebook Remove 'Fake News' Posts about False Death Tax Plans*, The Sydney Morning Herald (Apr. 19, 2019), https://perma.cc/U5J2-XTUB.

During this conversation, the Facebook executives said not all the material had failed fact checking, and in any case, fact checking applied only to general Facebook users, not to any content posted or promoted by politicians or parties. In any case, the social media giant did not want to play censor when it came to political claims.

Carroll was dissatisfied and said he wanted the matter escalated within the company. As the campaign entered the final week, some evidence emerged of a coordinated and well-financed effort to boost the messaging.

. . .

On 16 May, in response to Carroll's request for an escalation, Facebook put forward Simon Milner, the Singapore-based vice-president of the company in the Asia-Pacific. Milner reiterated the advice given by Garlick, but told Labor's digital team he would provide a report with some urgency on the concrete steps Facebook was taking to limit the damage.

Election day came and went, and Labor is still waiting for that report.

This week, Carroll wrote to Milner reminding him that he had promised to supply a report demonstrating "identifiable and measurable steps Facebook had taken to combat the spread of this specific misinformation campaign".

"I am yet to receive any information beyond a reference to a broad and generic second last week activity report which failed to list death tax as an issue being searched amongst several at all," the national secretary said in his letter.

Carroll wondered if Milner would be so kind as to advise when the report might be received.[82]

[82] Katharine Murphy, Christopher Knaus & Nick Evershed, '*It Felt Like a Big Tide': How the Death Tax Lie Infected Australia's Election Campaign*, The Guardian (June 7, 2019), https://perma.cc/X4U7-HSBN. See also Max Koslowski, *With One Click, the Liberals Inadvertently Unleashed the Ultimate Election Scare Campaign*, The Sydney Morning Herald (June 1, 2019), https://perma.cc/KA94-H56L.

Canada

Tariq Ahmad
Foreign Law Specialist

SUMMARY Currently there does not appear to be any law in Canada that expressly prohibits the dissemination of "fake news." Section 181 of Canada's Criminal Code prohibiting false news was declared unconstitutional by the country's high court. However, other offenses described in Canada's Criminal Code and Election Act may be relevant to the issue of fake news, such as an offense prohibiting false statements about a candidate for the purpose of influencing the outcome of an election. Canada has recently taken measures to ensure the integrity of the Canadian democratic process in advance of the October 2019 federal election. Canada's Digital Charter emphasizes the importance of democratic values and the protection of the country's electoral system. Consistent with that framework, the Canadian government is using a multitude of tools and modifying existing processes to enhance citizen preparedness, improve organizational readiness, combat foreign interference, and increase the proactivity and accountability of social networks in protecting Canadian democracy. In December 2018, Canada passed the Elections Modernization Act. Provisions in this Act stipulate that certain social networks must create and preserve registries of partisan advertising messages and election advertising messages posted on their respective platforms. Additionally, the government of Canada has pledged to invest Can$7 million in digital literacy programs before the federal election.

I. Background

In late March 2019, the Communications Security Establishment, Canada's national signals intelligence and cybersecurity agency, stated in a report that it is "very likely that Canadian voters will encounter some form of foreign cyber interference related to the 2019 federal election."[1] Expecting foreign disinformation during the election season, the government of Canada has taken measures to ensure the integrity of the country's democracy. These measures particularly target social media platforms and impose a higher level of accountability for social networks while calling for their cooperation with the government.

The problem of fake news has been well-documented. CBC/Radio Canada conducted a multi-year analysis of 9.6 million tweets from Twitter accounts that have since been deleted and found that "[r]oughly 21,600 tweets from those troll accounts," which were suspected to have originated from Russia, Iran, and Venezuela, "directly targeted Canadians—many of them with messages critical of Canadian pipeline projects and tweets that highlighted divisions over Canada's policies

[1] Canadian Centre for Cyber Security, *Executive Summary: 2019 Update: Cyber Threats to Canada's Democratic Process* (2019), https://perma.cc/G6G5-EDXY.

on immigration and refugees."[2] In addition, a 2019 survey[3] conducted by the market research firm Ipsos on behalf of the Centre for International Governance Innovation (CIGI), a nonpartisan think tank, found that "[n]inety per cent of Canadians say they have fallen for fake news online, with many listing Facebook as the most common source of misleading reports."[4] However, according to the poll, only 58% agreed with the claim that "fake news had a negative effect on their political discussions with family and friends."[5]

Attempts to address the problem of misinformation must be balanced against the right to freedom of expression protected by subsection 2(b) of the Canadian Charter of Rights and Freedoms, which provides that everyone has the fundamental freedom of "thought, belief, opinion and expression, including freedom of the press and the media communication."[6] Fundamental rights, including freedom of expression, are subject to section 1, which allows "reasonable" limits to be placed on those rights.[7] This means that "once an infringement of a Charter right has been established, the courts must decide whether the violation by the government or other institution to which the Charter applies can be considered justified."[8]

II. Current Legislation

Currently there does not appear to be any law in Canada that expressly prohibits the dissemination of false news "unless it is defamatory and covered by libel laws."[9] While section 181 of Canada's Criminal Code prohibits the spreading of false news,[10] Canada's Supreme Court held that the law was unconstitutional in *R v. Zundel* (1992)[11] because it violates section 2(b) (on

[2] Roberto Rocha & Jeff Yates, *Twitter Trolls Stoked Debates about Immigrants and Pipelines in Canada, Data Show*, CBC (Feb. 12, 2019), https://perma.cc/7P7Q-UX79.

[3] Ipsos Public Affairs, *CIGI-Ipsos Global Survey: Internet Security & Trust 2019 Part 3: Social Media, Fake News & Algorithms* (2019), https://perma.cc/X5RX-PL76.

[4] Elizabeth Thompson, *Poll Finds 90% of Canadians Have Fallen for Fake News*, CBC (June 11, 2019), https://perma.cc/2R9A-3AFT.

[5] Id.

[6] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act (1982), c. 11 (U.K.), § 2(b), https://perma.cc/2SZZ-TRYJ.

[7] Julian Walker, Parliamentary Info. & Research Serv., Pub. No. 2018-25-E, Library of Parliament, Legal and Social Affairs Division, *Hate Speech and Freedom of Expression: Legal Boundaries in Canada* 3 (June 29, 2018), https://perma.cc/8JPB-BMJ9.

[8] Id. at 2.

[9] Kathleen Harris, *MPs Look for Ways to Fight 'Fake News' In Wake of Mosque Shooting*, CBC (Feb. 2, 2017), https://perma.cc/SX23-TY6H.

[10] The provision, section 181 of the Criminal Code, R.S.C. (1985), c. C-46, https://perma.cc/7EDV-P7WF, states as follows:

> **Spreading false news**
>
> **181** Every one who wilfully publishes a statement, tale or news that he knows is false and that causes or is likely to cause injury or mischief to a public interest is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

[11] R. v. Zundel [1992] 2 SCR 731, https://perma.cc/7LJS-GCDA.

freedom of expression) of the Canadian Charter of Rights and Freedoms.[12] The section therefore has no legal effect or force and the government is in the process of removing this "zombie" provision.[13] However, Canada recently enacted the Elections Modernization Act to address the problem in the context of the country's elections.

There are other provisions in the Criminal Code that could apply more generally to situations of fake news, including section 372(1), which establishes an offense of "false information" where a person commits an offense if they convey "information that they know is false, or causes such information to be conveyed by letter or any means of telecommunication," with the "intent to injure or alarm a person."[14]

A. Prohibition on False Statements Aimed at Influencing Elections

The Elections Modernization Act, enacted in December 2017 and fully effective on June 13, 2019,[15] amended the Canada Elections Act (CEA)[16] and other acts to modernize Canadian election laws. According to a government press release, "[t]he new legislation is part of a comprehensive plan to safeguard Canadians' trust in our democratic processes and increase participation in democratic activities."[17]

Among the changes included in the Act was a provision making it an offense "to make false statements about a candidate for the purpose of influencing the outcome of an election."[18] Specifically, the Act provided as follows:

> **Publishing false statement to affect election results**
>
> **91 (1)** No person or entity shall, with the intention of affecting the results of an election, make or publish, during the election period,
>
> > **(a)** a false statement that a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party has committed an offence under an Act of Parliament or a regulation made under such an Act — or under an Act

[12] *R. v. Zundel: Case Analysis*, Global Freedom of Expression, Columbia U., https://perma.cc/RY9Q-SWCW.

[13] *Questions and Answers – An Act to Amend the Criminal Code (Removing Unconstitutional Portions or Provisions)*, Dep't of Justice, Gov't of Canada (last modified Mar. 9, 2017), https://perma.cc/7D69-Z62H; Alysha Hasham, *Purging Criminal Code of Defunct 'Zombie Laws' No Simple Task*, The Star (Jan. 1, 2017), https://perma.cc/3AVS-Z9AQ?type=image.

[14] Criminal Code, R.S.C. (1985), § 372(1).

[15] Elections Modernization Act, Bill C-76, First Session, Forty-Second Parliament, 64-65-66-67 Elizabeth II 2015-2016-2017-2018, Statutes of Canada 2018, ch. 31, https://perma.cc/HKT8-K8VW; see also *Bringing Bill C-76 into Force*, Elections Canada, https://perma.cc/3VVE-FG7Y.

[16] Canada Elections Act, S.C. 2000, c. 9, https://perma.cc/BSA3-R97Z.

[17] Press Release, Gov't of Canada, Government of Canada Passes Elections Modernization Act (Dec. 14, 2018), https://perma.cc/7RZE-CSXE.

[18] Joan Bryden, *Not Much Elections Canada Can Do about Fake News Spread about Candidates*, Nat'l Post (Feb. 7, 2019), https://perma.cc/YY44-Z7RT.

> of the legislature of a province or a regulation made under such an Act — or has been charged with or is under investigation for such an offence; or
>
> **(b)** a false statement about the citizenship, place of birth, education, professional qualifications or membership in a group or association of a candidate, a prospective candidate, the leader of a political party or a public figure associated with a political party.
>
> **Clarification**
>
> **(2)** Subsection (1) applies regardless of the place where the election is held or the place where the false statement is made or published.
>
> **Publishing false statement of candidate's withdrawal**
>
> **92** No person or entity shall publish a false statement that indicates that a candidate has withdrawn.[19]

However, according to a news report, this provision "applies quite narrowly to false statements about whether a candidate has broken the law or withdrawn from the election, as well as about a candidate's citizenship, place of birth, education, professional qualifications or membership in a group."[20]

B. Prevention of Foreign Interference in Elections

The Elections Modernization Act also aims to prevent foreign interference in the election process by amending the CEA with regard to paid political advertisements through online platforms.[21] Foreigners and foreign entities cannot buy regulated ads during the election period[22], which is now defined as a maximum of fifty days. The Act created a new pre-election period that started on June 30, 2019, and will end the day the election is called.[23]

Platform operators or owners can be prosecuted (or other compliance or enforcement actions can be taken) for knowingly selling election advertising to non-Canadians.[24] The Act prevents third parties from using funds for a regulated activity, including election advertising, if the source of funds is a foreign entity;[25] prohibits foreign third parties from participating in elections and incurring expenses for regulated activities (including partisan advertising expenses) that take

[19] Canada Elections Act §§ 91 & 92.

[20] Bryden, supra note 18.

[21] Elections Modernization Act, S.C. 2018, c. 31, https://perma.cc/A4F6-DKH9.

[22] Canada Elections Act, § 349.4 (1)(b).

[23] Rachel Aiello, *Vouching, Voter ID, Advertising: How New Elections Law Changes Impact You*, CTV News (June 12, 2019), https://perma.cc/TNG8-YEXL.

[24] *New Registry Requirements for Political Ads on Online Platforms*, Elections Canada (July 17, 2019), https://perma.cc/H877-PVUB.

[25] Canada Elections Act § 349.02.

place during the pre-election period and the election period;[26] and prohibits the selling of advertising space to foreigners who are unduly influencing electors.[27]

The Elections Modernization Act also imposes requirements on online platforms for better transparency and integrity of content during elections. Section 319 of the CEA defines an "online platform" as "an Internet site or Internet application whose owner or operator, in the course of their commercial activities, sells, directly or indirectly, advertising space on the site or application to persons or groups."[28] The threshold activity bringing a platform within the scope of the Act is set forth in section 325.1(1) of the CEA.[29]

Platforms in this category must maintain a digital registry of all regulated ads, publishing the registry and the names of the agents who authorized the ads.[30] Only federal elections are covered, but the provisions apply to both general elections and by-elections. Registered or eligible parties, registered associations, nomination contestants, potential candidates, and third parties that are required to register under sections 349.6(1) or 353(1) of the Act must include on the registry any partisan advertising and election advertising that was published on the platform during that period.[31] Subsection 325.1(3) describes the information to be included in the registry.[32] The registry must include an electronic copy of each partisan advertising message published on the platform.[33]

Ads are generally required to be included in the registry on the day they first appear on the platform, and each ad must be kept in the registry for two years following an election. After that, platform operators or owners must keep the registry information concerning an ad for another five years.[34]

---

[26] Id. §§ 349.4(1) & 351.1(1).

[27] Id. § 282.4 (5).

[28] Id. § 319.

[29] Per id. § 325.1(1), it encompasses platforms that,

> in the 12 months before the first day of the pre-election period, in the case of the publication on the platform of a partisan advertising message, or the 12 months before the first day of the election period, in the case of the publication on the platform of an election advertising message, was visited or used by Internet users in Canada an average of at least the following numbers of times per month: (a) 3,000,000 times, if the content of the online platform is available mainly in English; (b) 1,000,000 times, if the content of the online platform is available mainly in French; or (c) 100,000 times, if the content of the online platform is available mainly in a language other than English or French.

[30] *New Registry Requirements for Political Ads on Online Platforms*, supra note 24.

[31] Canada Elections Act § 325.1(2)

[32] Id. § 325.1(3)

[33] Id.

[34] *New Registry Requirements for Political Ads on Online Platforms*, supra note 24.

The Act also requires entities posting partisan advertising on a platform to provide the platform owner or operator the information needed to comply with the law.[35]

III. Other Government Actions

A. The Christchurch Call

In May 2019, Canadian Prime Minister Justin Trudeau announced that Canada would adopt the "Christchurch Call." The Christchurch Call is an initiative launched by New Zealand Prime Minister Jacinda Ardern and French President Emmanuel Macron two months after the live-streamed massacre in Christchurch, New Zealand. It is a commitment by governments and technology companies to eliminate terrorist and violent extremist content on the internet.[36] While acknowledging that "respect for freedom of expression is fundamental," the initiative asserts that "no one has the right to create and share" such content online.[37] Trudeau reportedly stated that social networks "have to step up in a major way to counter disinformation. And if they don't, we will hold them to account and there will be meaningful financial consequences."[38]

B. Canada's Digital Charter

On May 21, 2019, the Honorable Navdeep Bains, Minister of Innovation, Science and Economic Development, announced the introduction of Canada's Digital Charter, a commitment to building safer online spaces. [39] The Charter's ten principles reflect the concerns the government heard from Canadians during public consultations.

The Digital Charter's second principle addresses "safety and security" and stipulates that "Canadians will be able to rely on the integrity, authenticity and security of the services they use and should feel safe online." The eighth principle concerning a strong democracy addresses the issue of online advertising and disinformation.[40] With this principle, the government of Canada promises to "defend freedom of expression, and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions." The ninth principle calls for being "Free from Hate and Violent Extremism" so "Canadians can expect that digital platforms will not foster or disseminate hate, violent extremism or criminal content."[41]

---

[35] Canada Elections Act § 325.1(5)

[36] *Christchurch Call: To Eliminate Terrorist & Violent Extremist Content Online,* Christchurch Call, https://perma.cc/P7ZK-EAN4..

[37] Id.

[38] *Trudeau Warns of 'Meaningful Financial Consequences' for Social Media Giants that Don't Combat Hate Speech*, CBC (May 16, 2019), https://perma.cc/29GB-3GV2.

[39] Press Release, *Minister Bains Announces Canada's Digital Charter*, Innovation, Science and Economic Development Canada (May 21, 2019), https://perma.cc/9SJH-58BG.

[40] *Canada's Digital Charter: Trust in a Digital World*, Innovation, Science and Economic Development Canada, https://perma.cc/M24Q-UNPB

[41] Id.

The Digital Charter is principle-based and is therefore not a legally binding document. However, it is a clear indication that the government intends to make the integrity of information presented to Canadians on online platforms a priority.

C. Multi-Pronged Approach to Strengthening the Electoral System

The Canadian government has announced a multi-pronged approach to strengthening the electoral system against cyber-enabled threats in advance of the 2019 elections, which includes four pillars: (a) enhancing citizen preparedness, (b) improving organizational readiness, (c) combatting foreign interference, and (d) increasing the proactivity of social networks.[42]

1. Enhancing Citizen Preparedness

Canada's government has implemented the Critical Election Incident Public Protocol, a nonpartisan process that seeks to inform Canadians of threats to the integrity of the 2019 General Elections.[43] The Cabinet Directive on the Critical Election Incident Public Protocol[44] includes provisions for informing candidates, organizations, and elections officials if they have been the known target of an attack, and also briefing and informing the prime minister and other high-level officials that a public announcement is planned and of the process for informing the public.[45] An experienced panel of high-ranking Canadian public officials is then responsible for determining whether the threshold for informing Canadian citizens of such incidents has been met, based on information presented by Canada's various national security agencies. Numerous variables are considered in making this determination, including an incident's ability to undermine a free and fair election, its potential to undermine the credibility of the election process, and the degree of confidence officials have in the intelligence or information about the incident. If the threshold is deemed to have been met, the public is informed of steps to be taken for security purposes.[46]

Following an election, the Critical Election Incident Public Protocol calls for an assessment of its implementation. The report is to be presented to the prime minister and the National Security and Intelligence Committee of Parliamentarians. A version intended for the public must also be prepared.[47]

2. Improving Organizational Readiness

To deal with "[m]alicious foreign actors" who seek to undermine democratic societies and institutions, electoral processes, sovereignty, and security, the government has pledged to offer

[42] *Protecting Democracy*, Gov't of Canada (last modified July 25, 2019), https://perma.cc/J8N3-6UCZ.

[43] *Critical Election Incident Public Protocol*, Gov't of Canada (last modified July 9, 2019), https://perma.cc/T4XX-RVZP.

[44] Gov't of Canada, Cabinet Directive on the Critical Election Incident Public Protocol (July 9, 2019), https://perma.cc/R5MS-STCB.

[45] Id.

[46] Cabinet Directive on the Critical Election Incident Public Protocol, supra note 44, § 6.0

[47] Id. § 9.0.

technical advice and assistance regarding online security measures to political parties and election administrators, to help protect organizational cybersystems; sensitize decision makers to the nature of foreign interference; and provide classified threat briefings for key political party leaders.[48] Moreover, the Canadian Security Intelligence Service and the Communications Security Establishment are working with Elections Canada, the independent agency responsible for conducting federal elections, to identify threats, emerging tactics, and systems vulnerabilities.[49]

3. Combatting Foreign Interference

The Canadian government has announced the newly established Security and Intelligence Threats to Elections (SITE) Task Force, composed of already-existing organizations: the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, the Communications Security Establishment, and Global Affairs Canada.[50] The SITE Task Force is working to prevent covert, clandestine, and criminal activities from interfering with or influencing the electoral process in Canada by "building awareness of foreign threats to Canada's electoral process," and "preparing the Government to assess and respond to those threats."[51] In this regard, the government will analyze foreign social media activity to look at trends and identify Canadian vulnerabilities, and will also share knowledge and coordinate international responses through the G7 Rapid Response Mechanism established at the 2018 G7 Summit in Quebec, whereby the G7 nations "agreed to create a Rapid Response Mechanism to better coordinate the identification of and responses to evolving threats to our democracy. As the international lead of the G7 Rapid Response Mechanism, Canada will manage, triage, share information and identify opportunities for a joint G7 response to threats to democratic processes."[52]

4. Making Social Networks Proactive

The Canadian Government acknowledges the crucial role that social media and digital platforms have in promoting a healthy democracy.[53] Minister of Democratic Institutions Karina Gould has therefore begun discussions with social media companies. Social networks are expected to be transparent when political advertising is posted on their respective platforms. They must combat any form of manipulation used for antidemocratic purposes.

To further reinforce this responsibility, the Canadian government has released Canada's Declaration on Electoral Integrity Online.[54] The Declaration states that "[s]ocial media and other

---

[48] *Improving Organizational Readiness*, Gov't of Canada (last modified Jan. 30, 2019), https://perma.cc/GV7P-3FBA.

[49] Id.

[50] *Combatting Foreign Interference*, Gov't of Canada (last modified July 9, 2019), https://perma.cc/75A6-EWW3.

[51] Id.

[52] Id.

[53] *Expecting Social Platforms to Act*, Gov't of Canada (last modified July 9, 2019), https://perma.cc/D2WT-CMCW.

[54] *Canada Declaration on Electoral Integrity Online*, Gov't of Canada (last modified May 27, 2019), https://perma.cc/VK6D-83BZ.

online platforms and the Government of Canada recognize their respective responsibilities to help safeguard this fall's [October 2019] election and to support healthy political discourse, open public debate and the importance of working together to address these challenges head-on."[55] To this end the government and certain social media platforms commit to work together to address the integrity, transparency, and authenticity of content posted on social media platforms in the lead-up to the 2019 federal elections. The Declaration specifies that digital platforms must

- apply their latest advancements and most effective tools for the protection of Canadian democratic processes;
- promote safeguards and protect against misrepresentation of candidates, parties, and other key electoral officials;
- have a government point of contact;
- regulate political advertising by helping users know when and why they are seeing political ads;
- make terms and conditions easily accessible and enforce them in a fair, consistent, and transparent manner;
- continuously remove fake accounts and inauthentic content; and
- help users better understand the sources of advertising they are seeing.[56]

As of May 2019, Facebook, Microsoft, and Google had signed onto the Declaration.[57]

5. Digital Literacy Programs

In January 2019, the Canadian government announced plans to spend Can$7 million on combatting disinformation, specifically by investing in digital, news, and civic literacy programming.[58] Minister Gould announced a campaign that would educate the public about content deemed "misinformation" by the government. She elaborated that "citizens who recognize fraud, misinformation and manipulation when they see it online are less likely to fall victim to it."[59] The funding is to be distributed among organizations heading digital-literacy programs to help Canadian voters better assess online content and increase their understanding of disinformation.[60] The objective is to encourage Canadians to read a diversity of sources, think

[55] Id.

[56] Id.

[57] Joan Bryden, *Several Tech Giants Sign onto Canadian Declaration on Electoral Integrity*, Global News (May 27, 2019), https://perma.cc/A5LL-UAV6.

[58] Rachel Aiello, *Feds Unveil Plan to Tackle Fake News, Interference in 2019 Election*, CTV News (Feb. 27, 2019), https://perma.cc/6275-SLSL.

[59] Alex Boutilier, *Federal Liberals Tap Senior Bureaucrats to Warn Canadians of Election Meddling*, The Star (Jan. 30, 2019), https://perma.cc/DXL2-WH29.

[60] Id.

before they share online content, and question the trustworthiness of sources.[61] Further details regarding the campaign and initiatives by the government have not been revealed to the public.

IV. Media Coordination

Social networks have reacted differently to the mandatory requirement of preserving registries for political advertisements. Some have decided to eliminate political advertisements on their platforms altogether in order to avoid the risk of not conforming to the law.

- Microsoft has decided to ban all political advertisements on all its platforms, including MSN and Bing.[62]
- Google expressed opposition to the Elections Modernization Act well before it was enacted. The company argued that the creation of registries was unachievable as it would require changing its entire online advertising infrastructure.[63] Therefore, Google has banned political advertisements ahead of the next Canadian federal election.[64] Instead, it plans to focus on Canadian literacy programs and connecting people to relevant and useful information.
- Reddit released an official statement informing the public that it will not accept online advertisements before the upcoming Canadian federal election.[65]
- Facebook decided to comply with the new law's registry requirements, viewing it as an opportunity to democratize digital marketing. Facebook is creating a new advertisement library that will capture details about the political ads on its platform.[66] It believes its registries will exceed the standards of the law. Facebook has also started to label ads as "political" and inform readers of the person or entity paying for them. However, according to one news report, Facebook says "most advertisers identify the sponsors truthfully," and the company "does not verify this information unless it is reported to be false."[67]

Other platforms, such as LinkedIn and the Weather Network, have yet to publicize their strategy on how they plan to address fake news.[68]

---

[61] Aiello, supra note 58.

[62] Elizabeth Thompson, *Most of Canada's Top Websites Won't Post Federal Election Ads This Year*, CBC News (May 1, 2019), https://perma.cc/99XE-GPR5.

[63] Howard Solomon, *Google, Twitter Object to Proposed Canadian Online Platform Ad Registries*, IT World Canada (Nov. 30, 2018), https://perma.cc/73UB-MTML.

[64] David George-Cosh, *Google Bans Political Ads Ahead of Next Canadian Federal Election*, BNN Bloomberg (Mar. 5, 2019), https://perma.cc/B5KQ-2D43.

[65] Thompson, supra note 62.

[66] Id.

[67] Madeline Purdue, *Facebook Expands Political Advertising Disclaimers and Authorization to Canada and Ukraine*, USA Today (last updated June 25, 2019), https://perma.cc/A965-AKDM.

[68] Thompson, supra note 62.

China

Laney Zhang
Foreign Law Specialist

SUMMARY Despite the country's strict regulation of media and the internet, misinformation still appears to be permeating social media and the internet in China. Chinese law prohibits any online publication and transmission of false information that may disrupt the economic or social order. The law also bans other information, such as information that may endanger national security, overturn the socialist system, or infringe on the reputation of others. Spreading false information that seriously disturbs public order through an information network or other media is a crime punishable by up to seven years in prison.

Network operators are obligated to monitor the information disseminated by their users. Once a network operator discovers any information that is prohibited by law or regulation, it must immediately stop the transmission of such information, delete it, take measures to prevent it from proliferating, keep relevant records, and report to the competent government authority.

Social media platforms must maintain a license to operate businesses in China. Users are also required to register their real names and other identity information with service providers. Also, specific rules regulating internet news information services have been established. For example, when reprinting news, internet news information service providers may only reprint what has been released by official state or provincial news organizations, or other news organizations prescribed by the state.

I. Background

Although the Constitution of the People's Republic of China (PRC or China) declares that citizens enjoy freedom of speech and freedom of the press, these freedoms are not institutionally protected in practice.[1] Freedom House's 2019 *Freedom in the World* report states China is "home to one of the world's most restrictive media environments and its most sophisticated system of censorship, particularly online."[2]

Despite the strict regulation of the media and internet, misinformation, or what Chinese laws and domestic media often refer to as "rumors," still appears to be permeating the internet and social media in China. Internet regulators reportedly received 6.7 million reports of illegal and false information in a single month in July 2018, with many of the cases coming from Chinese social media platforms Weibo and WeChat.[3] The government has been dealing with online

[1] Qianfan Zhang, *The Constitution of China: A Contextual Analysis* 225 (2012).

[2] Freedom House, *Freedom in the World 2019: China Country Report*, https://perma.cc/GXC4-6NT6.

[3] Stella Qiu & Ryan Woo, *China Launches Platform to Stamp Out 'Online Rumors'*, Reuters (Aug. 30, 2018), https://perma.cc/3976-TPRB.

misinformation since the spread of the internet in the late 2000s, and has launched a series of campaigns to combat online rumors.[4]

Various factors are propelling the phenomenon of the spread of misinformation in China, a *Foreign Policy* article argues, such as "a deep sense of societal insecurity, the increasing politicization and commercialization of information, and a craving for self-expression." [5] According to the article, "the party-led campaigns against rumors have been seen as attempts to take out potential critics and enemies. When the government labels something a rumor, that information comes to be seen not as fake but as something the government doesn't want the public to know."[6]

II. Current Legislation

China does not have a law specifically regulating online political advertisement. The country's Cybersecurity Law, as discussed below, prohibits the publication and transmission of false information that may disrupt the economic or social order online, including through social media. The law also bans a wide range of other information, such as information that may endanger national security, overturn the socialist system, or infringe on the reputation of others.

A. Publication and Transmission of Prohibited Information

1. Prohibited Information

On November 7, 2016, China's first-ever Cybersecurity Law was adopted by the Standing Committee of the National People's Congress (NPCSC).[7] The Law prohibits network users from conducting a series of activities online, including

- endangering national security, national honor, or national interests;
- inciting subversion of national sovereignty or the overthrow of the socialist system;
- inciting separatism or breaking national unity;
- advocating terrorism or extremism;
- advocating ethnic hatred or ethnic discrimination;
- spreading violent or obscene information;

[4] Maria Repnikova, *China's Lessons for Fighting Fake News*, Foreign Policy (Sept. 26, 2018), https://perma.cc/U2N4-KKQ6.

[5] Id.

[6] Id.

[7] PRC Cybersecurity Law (adopted by the Standing Committee of the National People's Congress (NPCSC) on Nov. 7, 2016, effective June 1, 2017) (in Chinese), https://perma.cc/3HAP-D6MZ.

- fabricating or disseminating false information to disrupt the economic or social order; and
- infringing on the reputation, privacy, intellectual property, or other lawful rights and interests of others. [8]

2. Network Operators' Obligation to Stop Transmission and Delete Information

Network operators are obligated to monitor the information disseminated by their users. Once a network operator discovers any information that is prohibited by law or regulation, it must immediately stop the transmission of such information, delete the information, take measures to prevent the information from proliferating, keep relevant records, and report to the competent government authority.[9]

3. Penalties

Publication or transmission of the above-mentioned prohibited information specified by the Cybersecurity Law, or of any information that is prohibited from publication or transmission under other laws or administrative regulations, is subject to prescribed penalties.[10] According to the Cybersecurity Law, violation of the Law may result in administrative penalties and criminal sanctions.[11]

On August 29, 2015, the NPCSC adopted the Ninth Amendment to the PRC Criminal Law.[12] The Amendment added into the Law the crime of spreading false information that seriously disturbs the public order through an information network or other media. This offense is punishable by up to seven years in prison. The Ninth Amendment added a paragraph to article 291a of the Criminal Law, stating that

> [w]hoever fabricates false information on [a] dangerous situation, epidemic situation, disaster situation or alert situation and disseminates such information via [an] information network or any other media, or intentionally disseminates [the] above information while clearly knowing that it is fabricated, thereby seriously disturbing public order, shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention or public surveillance; if the consequences are serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years.[13]

[8] Id. art. 12, para 2.

[9] Id. art. 47.

[10] Id. art. 70.

[11] Id. art. 74.

[12] Ninth Amendment to the PRC Criminal Law (adopted by the NPCSC on Aug. 29, 2015, effective Nov. 1, 2015) (in Chinese), https://perma.cc/JZL6-XV2K, English translation available at Westlaw China (by subscription).

[13] Id. art. 32.

B. Internet Service Providers' Obligations to Cooperate

1. License Control

Social media platforms must maintain a license to operate businesses in China. According to the Administrative Measures on Internet Information Services, a regulation issued by the State Council on September 25, 2000, any service providing information to online users via the internet is subject to the regulation.[14] According to the regulation, profit-making internet service providers must obtain an operating license from government authorities. Nonprofit providers must also register with government authorities.[15]

The regulation sets forth obligations of the internet information service providers to cooperate with the government authorities. For example, service providers must keep records of all information published and the publication time, as well as users' information such as their accounts, IP address or domain name, time spent online, etc. Such records must be kept for sixty days and provided to competent government authorities when requested.[16]

2. Real-Name Registration

Social media users are also required by law to register their real names and other identity information with service providers. Under the Cybersecurity Law, when providing services of information publication or instant messaging, the service providers must ask users to register their real identity information. The service providers are prohibited from providing relevant services to any users who do not perform the identity authentication steps.[17]

Where service providers fail to authenticate users' identities, the competent authorities may order them to rectify their wrongdoing, suspend their businesses, shut down their websites, revoke relevant licenses, or impose a fine of 50,000 to 500,000 yuan (about US$7,500 to $75,000) on the service providers and/or a fine of 10,000 to 100,000 yuan (about US$1,500 to $15,000) on the responsible persons.[18]

C. Specific Rules on Internet News Information Services

On the basis of the PRC Cybersecurity Law and the Administrative Measures on Internet Information Services, China's central internet information authority, the Cyberspace

[14] State Council, Administrative Measures on Internet Information Services (Sept. 25, 2000, effective on the same day) art. 2 (in Chinese), https://perma.cc/M6J4-HV7V.

[15] Id. art. 4.

[16] Id. art. 14.

[17] PRC Cybersecurity Law (adopted by the NPCSC on Nov. 7, 2016, effective June 1, 2017) art. 24 (in Chinese), https://perma.cc/3HAP-D6MZ.

[18] Id. art. 61.

Administration of China, issued the Provisions on Administration of Internet News Information Services on May 2, 2017.[19]

1. License Control

Under the Provisions, any entities providing internet news information services to the public—whether through websites, apps, online forums, blogs, microblogs, social media public accounts, instant messaging tools, or live broadcasts—must obtain a license for internet news information services and operate within the scope of the activities sanctioned by the license.[20] Such licenses are only issued to legal persons incorporated within the territory of the PRC, and the persons in charge and editors-in-chief must be Chinese citizens.[21]

Providing internet news information services without a proper license is punishable by a fine of 10,000 to 30,000 yuan (about US$1,500 to $4,500).[22]

2. Restrictions on Reprinting News

When reprinting news, internet news information service providers may only reprint what has been released by official state or provincial news organizations, or other news organizations prescribed by the state. The original sources, authors, titles, and editors must be indicated to ensure that the sources of the news are traceable.[23]

State or local internet content authorities may issue a warning to violators of this provision, order them to rectify their wrongdoings, suspend their news services, or impose a fine of 5,000 to 30,000 yuan (about US$750 to $4,500). Violators may also be criminally prosecuted, according to the Provisions.[24]

3. Prohibited Information

The Provisions also prohibit internet news information service providers and users from producing, reproducing, publishing, or spreading information content prohibited by applicable laws and administrative regulations.[25] State or local internet content authorities may issue a warning to violators of this provision, order them to rectify their wrongdoings, suspend their news services, or impose a fine of 20,000 to 30,000 yuan (about US$3,000 to $4,500). Violators may also be criminally prosecuted, the Provisions state.[26]

---

[19] Cyber Administration of China, Provisions on Administration of Internet News Information Services (May 2, 2017, effective June 1, 2017) art. 1 (in Chinese), https://perma.cc/Y5VB-XZJV.

[20] Id. art. 5.

[21] Id. art. 6.

[22] Id. art. 22.

[23] Id. art. 15(1).

[24] Id. art. 24.

[25] Id. art. 16(1).

[26] Id. art. 25.

4. Obligations of Service Providers

Once internet information service providers find any content prohibited by the Provisions or other laws and administrative regulations, they must immediately stop transmitting the information, delete the information, keep the relevant records, and report the matter to competent government authorities.[27]

The Provisions also repeat the requirement of real-name registration under the Cybersecurity Law, providing that internet news information service providers must ask users of the internet news information publication platform service to register their real names and provide other identity information.[28]

Violators of these provisions are punishable by the state or local internet information authority in accordance with the Cybersecurity Law.[29]

III. Other Government Actions

The government has reportedly launched campaigns to combat online rumors by shutting down social media accounts, demanding that websites "rectify their wrongdoing," detaining those accused of manufacturing misinformation, and imposing penalties on dissenters and opinion leaders.[30]

In 2018, China launched a platform named "Piyao"—a Chinese word meaning "refuting rumors."[31] The platform, which also has a mobile app and social media accounts, broadcasts "real" news sourced from state-owned media, party-controlled local newspapers, and various government agencies.[32]

IV. Media Coordination

Tencent, the operator of China's biggest social media platform WeChat, released a report in January 2019 concerning its fight against rumors spread online. According to the report, WeChat intercepted over 84,000 rumors in 2018. In addition, thousands of "anti-rumor articles" were published on WeChat by government internet, public security, and food and drug authorities; scientific research institutions; and the state media.[33]

---

[27] Id. art. 16(2).

[28] Id. art. 13(1).

[29] Id. art. 26.

[30] Repnikova, supra note 4.

[31] Homepage, China Internet Joint Rumor Refuting Platform (in Chinese), https://perma.cc/JN4X-F8UA.

[32] Qiu & Woo, supra note 3.

[33] *2018 Report on Managing Online Rumors Published, 774 Institutions Refuted Rumors on WeChat*, People.cn (Jan. 18, 2019) (in Chinese), https://perma.cc/8QCK-37ZQ.

The *Foreign Policy* article, which was published in September 2018, reports more incidents where social media companies cooperated with the government to fight the spread of "rumors:"

> In 2016, Beijing requested that Baidu delete unverified advertisements, revise its procedures for running paid listings, and provide reimbursements for losses caused by the promotion of fake news. Last year, the country's national and provincial cyberspace authorities investigated top social networking platforms, including WeChat, Weibo, and Baidu Tieba, and found posts containing "violence, terror, rumors and obscenity." The companies, in turn, offered apologies, self-criticism, and more self-regulation. This June, the authorities demanded that the internet search engine Sogou delete advertisements of the popular video app Douyin, which allegedly "insulted heroes and martyrs."[34]

[34] Repnikova, supra note 4.

Denmark

Elin Hofverberg
Foreign Law Specialist

SUMMARY Denmark considers nontransparent political advertising online a possible threat to democracy. Denmark protects free speech both in its Constitution and through its international obligations. In 2019, Denmark amended its law on foreign influence on domestic public opinion to include social media. The crime of influencing public opinion on behalf of a foreign government now carries a twelve-year term of imprisonment if carried out during elections. In 2018, the government announced eleven initiatives to combat disinformation, including requiring greater transparency in political advertising, as well as collaborations between the government and media, especially on media literacy. The Danish media industry has launched a labeling tool whereby media members can mark their websites to indicate that they are subject to the Press Council rules on media conduct.

I. Background

A. Dissemination of Disinformation Using Social Media

Denmark recognizes the mass dissemination of disinformation and misinformation through social media as a threat. Denmark is especially cognizant of fake news from Russia, which the Danish defense minister, together with the defense minister of Sweden, described as a problem in a joint op-ed in 2017.[1] Others argue that fake news is not as much of a problem as misinformation caused by commercial journalism and entertainment.[2] However, a majority of the Danish people still consider state and traditional media to be "free from political or commercial pressure,"[3] indicating that Danes still view these types of media as independent, and unlikely to spread misinformation or disinformation. The use of social media is on the rise in Denmark and in 2018 a majority of persons aged sixteen to eighty-nine used Facebook on a daily basis.[4] A majority of persons aged sixteen to twenty-four also used YouTube, Snapchat, and Instagram on a daily basis.[5]

[1] Peter Hulltqvist & Claus Hjort Frederiksen, Op-ed, *Ryska 'fake news' - en fara för våra länder*, Aftonbladet (Aug. 30, 2017), https://perma.cc/A5ZZ-ZJJ9.

[2] Rasmus Kerrn-Jespersen, *Fake news er ikke problem i Danmark – men misinformation er*, Mandag Morgen (Jan. 1, 2018), https://perma.cc/ALK8-4MBX.

[3] European Commission, *Special Eurobarometer 452 Report Media Pluralism and Democracy* (2016), https://perma.cc/T7P7-FC9J.

[4] *Mediernes Udvikling i Danmark*, Kulturministeriet, https://perma.cc/GG6V-MWYW.

[5] Id.

The Danish Defense in 2017 published an evaluation of international actions that had an impact on Danish security.[6] In the report, disinformation and influence campaigns using social media were recognized as threats to Denmark.[7] The report specified that Russia, ever since the Cold War, has believed that internal tensions within a country increase the level of influence that Russia exercises over the rest of the world.[8] As technology has increased, the use of social media to attain these goals is thus instrumental.[9] Moreover, the Danish Defense point to how influence campaigns become harder to spot as the statements "appear to have no state affiliation and [in] social media activities [the] Russian origin has been disguised."[10] The Danish Defense also notes that other groups, such as militant Islamists, use social media for propaganda purposes.[11] The Danish Security and Intelligence Police (Politiets Efterretningstjeneste, PET) also singled out social media as a vessel for fake news and rumors.[12]

B. Principles of Free Speech

Freedom of speech and freedom of the press are protected in the Danish Constitution:[13]

> Every person shall be at liberty to publish their ideas in print, in writing, and in speech, subject to liability in a court of law. Censorship and other preventive measures may never again be introduced.[14]

In addition, freedom of speech is protected in the European Convention on Human Rights, to which Denmark is a party.[15] Denmark has, however, passed laws that limit free speech and it also permits the blocking of certain websites.[16]

---

[6] Forsvarets Efterretningstjeneste (FE), *Efterretningsmæssig Risikovurdering 2017 En aktuel vurdering af forhold i udlandet af betydning for Danmarks sikkerhed* (2017), https://perma.cc/8WT9-86QQ (original in Danish), https://perma.cc/7973-U68F (English translation).

[7] Id. at 12 (original Danish version).

[8] Id. at 20. Denmark has previously had controversies with Russia, for example there have been reports that Russia hacked into Danish Foreign Ministry accounts in 2017. Martin Borre & Thomas Larsen, *Russia Hacked into Danish Defence Emails for Two Years, Intelligence Report Reveals*, Berlingske (Apr. 23, 2017), https://perma.cc/GZ2C-LHUH.

[9] FE, supra note 6.

[10] Id. at 20 (English translation).

[11] Id. at 36.

[12] PET, *Årlig redegørelse 2017* [*Annual Report 2017*], https://perma.cc/JY53-JNMJ.

[13] § 77 Danmarks Riges Grundlov (Grundloven) [Danish Constitution], https://perma.cc/EGX2-XLXS.

[14] Id. (translation by author).

[15] European Convention on Human Rights, Nov. 4, 1950, 213 U.N.T.S. 221, https://perma.cc/Y584-N9KT.

[16] See below, Part II.

II. Legislation

A. General Rules on Advertisements Online

Danish law prohibits covert marketing, i.e. marketing should be distinguishable as advertisements, compared to editorial information in a newspaper.[17]

The Danish Consumer Ombudsman has published Guidelines for advertisements that are made using social media.[18] The Guide mainly targets product placement by "influencers" (bloggers, Instagrammers, etc.), but the principle applies to all advertisements.[19] Thus, an advertisement should be distinguishable as an advertisement and it should be clear who sponsored the ad or its content.[20]

B. Limits on Political Advertisements

1. Danish Legislation

Political advertisements may not be broadcast on television or public radio in Denmark.[21] Danish politicians have criticized the current rules, which do not specifically prohibit political advertisements on streaming services (such as TV2 Play, or Viafree) but prohibit the same content on live television, and in 2018 discussed expanding the prohibition to also include streaming services.[22] During the 2019 election campaign political campaigns were made available online on TV2, TV3, and Kanal 5 in connection with their streaming services.[23] No proposals have been made to prohibit political advertisements online generally, or on social media specifically. Politicians continue to use the internet for advertising purposes. For instance the Danish politician Joachim B. Olsen reportedly published advertisements on a Canadian porn site.[24]

---

[17] See also *Covert advertising*, Danish Consumer Ombudsman, https://perma.cc/H4RX-8SHA.

[18] *Skjult reklame på sociale medier*, Forbrugerombudsmanden, https://perma.cc/L3BD-KDD7; Forbrugerombudsmanden, *Gode råd til influenter om skjult reklame*, https://perma.cc/B5UU-BCFG.

[19] Forbrugerombudsmanden, *Gode råd til influenter om skjult reklame*, supra note 18.

[20] Id.

[21] § 76 stk. 3 Bekendtgørelse af lov om radio- og fjernsynsvirksomhed [Law on Radio and Television Broadcasts] (LBK nr 248 af 16/03/2019), https://perma.cc/RBP4-6P8E; § 14 Reklamebekendtgørelsen (BEK nr 801 af 21/06/2013), https://perma.cc/2V6J-QZHA. See also *Regler for politisk reklame*, Kulturministeriet, https://perma.cc/Z9TC-DMLY. Danish industry representatives have argued that political advertisement should be allowed on TV. *Det skal være tilladt med politiske reklamer på TV*, Dansk Erhverv, https://perma.cc/7BQZ-2J4W.

[22] Louise Reseke & Nicoline Lärka Sørensen, *Partier kritiserer åben dør for politiske reklamer på streamingtjenester*, Mediawatch (Nov. 23, 2018), https://perma.cc/X32U-5RCZ.

[23] Andreas Krog, *Partier ikke klar til politiske reklamer på flow-tv*, Altinget (June 4, 2019), https://perma.cc/985H-JY3B.

[24] Martin Selsoe Sorensen, *Danish Politician Puts Ad on Pornhub, Seeking Voters 'Where They Are'*, N.Y. Times (May 19, 2019), https://perma.cc/K3AU-TLNT.

2. EU Code of Practice on Disinformation

The European Union has adopted an EU Code of Practice on Disinformation that applies to Denmark as an EU Member State.[25] Several large media platforms have voluntarily signed up to be bound by the Code.[26] Thus, in the future Danish politicians will have to be authorized before placing political ads on Facebook in order to comply with the new Facebook user rules.[27] Facebook also requires a clear indication of who paid for an advertisement in cases where a politician received funding to cover the cost of the advertisement.[28]

3. Political Advertisement Tracker

In 2017, Information.dk (the website of the newspaper *Dagbladet Information*) launched a project together with ProPublica whereby the content of political advertisements related to the municipal election was tracked on Facebook by downloading all ads that users who subscribed to the service saw and thereafter sorting them as political and nonpolitical.[29] According to Information.dk, the service also provided a function whereby users could see the political advertisements that were not targeted towards them by clicking "advertisements that I cannot see."[30]

C. Criminal Sanctions on Political Propaganda

1. Hate Speech and Propaganda

Disseminating false information is not in of itself a crime in Denmark, and typically false statements are covered by the right to free speech. However, disseminating certain false information such as with respect to the value of financial instruments is specifically prohibited.[31] In addition, Denmark criminalizes defamation, insults, persecution (*forfølgelse*), and hate speech.[32]

[25] See European Union survey in this report.

[26] EU Code of Practice on Disinformation (2018), https://perma.cc/T9CX-9755; *Code of Practice on Disinformation*, European Commission (Sept. 26, 2018), https://perma.cc/SE58-9Z3P; Press Release, European Commission, Code of Practice on Disinformation (Sept. 26, 2018; last updated June 17, 2019), https://perma.cc/8MZK-97Z5; see also Jenny Gesley, *European Union: Commission Proposes EU-Wide Code of Practice to Combat Fake News Online*, Global Legal Monitor (May 11, 2018), https://perma.cc/3QKF-6N7M; Press Release, European Commission, A Europe that Protects: The EU Steps Up Action against Disinformation, (Dec. 5, 2018), https://perma.cc/8Y4R-2HZ4.

[27] *Nye krav til politiske reklamer på Facebook*, MediePlan (Mar. 29, 2019), https://perma.cc/VKZ6-SLBW.

[28] Id.; see also *Ads About Social Issues, Elections or Politics*, Facebook, https://perma.cc/437M-F8QE.

[29] Sebastian Gjerding, *Vær med til at kortlægge politiske reklamer på Facebook*, Information (Nov. 9, 2017), https://perma.cc/BYT7-USRD.

[30] Id. (translation by author).

[31] § 296 Straffeloven [Criminal Act] (LBK nr 1156 af 20/09/2018), https://perma.cc/VQ3P-JPJS.

[32] §§ 266b, 266c, 267 Straffeloven.

In 2017, the Danish Parliament repealed its then 334-year-old blasphemy law, which criminalized the public insult of religion, such as the burning of holy texts.[33] Denmark still criminalizes public speech that ridicules groups of persons of a certain faith, as well as persons belonging to a particular "race, skin color, national or ethnic origin, sexual orientation."[34] Engaging in such speech for propaganda purposes is considered an aggravating factor.[35] Section 226 of the Criminal Act states as follows:

> § 266 b. A person who publicly, or with the intent of dispersal in a wider circle, makes a statement or other message by which a group of persons is threatened, ridiculed, or degraded because of race, skin color, national or ethnic origin, faith, or sexual orientation, is punished with a fine or imprisonment of up to two years.[36]
>
> Stk. 2. During sentencing it shall be deemed an aggravating circumstance, if [the activity] has the characteristics of being propaganda activity.[37]

Having a propaganda intent means that "the activity [is undertaken] with the goal of influencing public opinion."[38] The use of a medium that facilitates dispersal to a wide circle is critical in the determination of whether the statement also violates the propaganda provision.[39] For example, the publication in a newspaper of an ad by members of a political youth organization that made derogatory comments about Muslims, who also published the same ad online, was punished with a fourteen-day term of imprisonment for the spreading of propaganda.[40] On the other hand, the publication of a song derogatory to Jews and Turks online was not considered propaganda, but rather hate speech.[41] In that case the speedy removal of the song from the website and the fact that no other similar songs had been published on the website led to the conclusion that it was only hate speech rather than propaganda.[42] In the first case the youth group had also printed 1,000 posters with the same message.[43]

---

[33] Lov om ændring af straffeloven [Law on Amending the Penal Code] (LOV nr 675 af 08/06/2017), https://perma.cc/2KT4-XWSN. For more information see Elin Hofverberg, *Denmark: Blasphemy Law Repealed*, Global Legal Monitor (July 6, 2017), https://perma.cc/85G4-J4EQ.

[34] § 266b Straffeloven. However, simply burning the Bible or the Koran would not be enough to be convicted of hate speech as defined in § 266b.

[35] Id. § 266b stk. 2.

[36] Id. § 266b (translation by author).

[37] Id. § 266b stk. 2 (translation by author).

[38] See 4 Michael Hansen Jensen et al., *Karnov Lovsamling* 6421 (34th. ed. 2018).

[39] Id.

[40] U 2003 1947 Ø, summary available in Jensen et al., supra note 38, at 6420.

[41] U 2003 2559, summary available in in Jensen et al., supra note 38, at 6420.

[42] Id.

[43] U 2003 1947 Ø, supra note 40.

2. Criminalization of Foreign Influence on Public Opinion

In addition to hate speech and defamation, Denmark also criminalizes speech that constitutes "unlawful influence activities" by foreign governments.[44] In 2019, Denmark amended its Criminal Act, thereby expanding unlawful influence activities to include activities that affect public opinion generally.[45] The law also prohibits efforts to influence European parliamentary elections.[46] In adopting the legislation, Denmark acknowledged that influence campaigns are a growing problem for Western countries, including Denmark.[47] The amended legislation requires for culpability that the illegal action "aids or enables a [foreign state actor]" to influence public opinion in Denmark.[48] Comments and posts published on Facebook therefore do not qualify, as Facebook is not considered a foreign power.[49] The law has been criticized by Jorn Vestergaard, professor of Criminal Law at Copenhagen University, who argues that it will limit "free, open, and critical public debate."[50] Violations carry a maximum of twelve years' imprisonment if carried out in connection with a national election, such as the Danish parliamentary election or the EU parliamentary election.[51] The purpose of the law was to "strengthen the criminal protections against foreign influence campaigns against Denmark," in view of rising levels of foreign influence campaigns in the country.[52]

3. No Criminalization of Use of "Bots"

The use of bots is not criminalized in Denmark. When proposing changes to the provision on foreign influence activities discussed in Part II(B)(2), above, the proposal included reference to the use of bots by foreign governments but did not extend so far as to prohibit their use.[53]

4. Blocking of Webpages that Sponsor Terrorism

Under Danish law, public access to websites may be blocked "if there are grounds to believe" that there are violations of Criminal Act sections 114-114i, 119, or 119a.[54] Thus, a website may be

[44] § 108 Straffeloven.

[45] Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed) [Act on Amendments to the Criminal Act (Unlawful Influence Activities)] (LOV nr 269 af 26/03/2019), https://perma.cc/Y4US-BTH3.

[46] Id.

[47] Lovforslag nr L95, Forslag til Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed), at 2, https://perma.cc/BZ9Y-H8PX.

[48] Id. at 3.

[49] Id. at 8. Compare with UfR2002.936 Ø, where a Danish customs agent was sentenced to four months of imprisonment in 1989 for having provided DDR officials with information on the Danish customs structure.

[50] Retsudvalget 2018-19L 95 Bilag 10, Offentlig, Kriminalisering af påvirkningsvirksomhed – kritik af lovforslag L 95, https://perma.cc/LA2Z-BRVG.

[51] Tillæg A Til lovforslag nr. L 95, Skriftlig fremsættelse (Nov. 14, 2018), https://perma.cc/2KVQ-4SNW.

[52] Lovforslag nr. L95, supra note 47, at 2.

[53] Justitsminister Søren Pape Poulsen, Forslag til Lov om ændring af straffeloven (Ulovlig påvirkningsvirksomhed) (Nov. 14, 2018), https://perma.cc/2UEL-88UX.

[54] § 791d Retsplejeloven [Judicial Procedure Act] (LBK nr 1284 af 14/11/2018), https://perma.cc/4C9S-KHFR.

blocked if there are grounds to believe its content promotes or sponsors terrorism.[55] The actual access prevention is ensured through DNS-blocking, i.e. the internet supplier blocks access, based on police requests.[56]

III. Other Government Actions

A. Creation of Action Plan and Task Force

In 2018, the Danish government ministries joined forces in an interdepartmental task force.[57] It listed eleven initiatives, including training of Ministry of Foreign Affairs communications staff in countering misinformation.[58] In addition, the list of initiatives included measures such as inviting representatives from the social medial platforms for a dialogue on how to handle foreign attempts to influence the Danish elections.[59] The Ministry for Foreign Affairs noted that

> influence campaign[s] can for instance include attempts to spread untrue information and stories in the media or to create a distorted coverage of a topic in order to influence an important political decision. These kind of campaigns are often designed to create discord amongst the population and seek to undermine the trust in for instance elections or public institutions.[60]

B. Command Center Against Misinformation

In accordance with the Action Plan presented by the Danish government in 2018, joint efforts by the Danish Security Intelligence Service and the Danish Defense Intelligence Service created a Command Center with the purpose of countering misinformation from foreign sources.[61] The initiatives provided that the agencies should collaborate in the following ways:

> 3. The Danish Security Intelligence Service (DSIS) and the Danish Defence Intelligence Service (DDIS) strengthen their focus on hostile foreign actors targeting Denmark with influence campaigns, including with regard to the upcoming parliamentary elections.
>
> 4. The Ministry for Economic Affairs and the Interior will in cooperation with DSIS and DDIS/The Centre for Cyber Security (CFCS) ensure that the necessary threat and vulnerability assessments are conducted in relation to the election.

---

[55] Id.; see also Justitsministeriet, Forslag til Lov om ændring af straffeloven, retsplejeloven og forskellige andre love (udkast) (2016-723-0069), https://perma.cc/PQ7X-JKTA, and *New Danish Law Can Lead to Substantial Internet Censorship*, EDRi (Jan. 25, 2017), https://perma.cc/J89E-LJ7T.

[56] See 3 Michael Hansen Jensen, *Karnovs Lovsamling* 5898 (34th ed. 2018).

[57] Press Release, Justitsministeriet, Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet (Sept. 7, 2018), https://perma.cc/3HST-QBNB; Press Release, Ministry of Foreign Affairs, Strengthened Safeguards against Foreign Influence on Danish Elections and Democracy (Sept. 7, 2018), https://perma.cc/WGH9-M2L3.

[58] Id.

[59] Id.

[60] Press Release, Ministry of Foreign Affairs, supra note 57.

[61] Id.

> 5. The Ministry for Economic Affairs and the Interior's response with regard to the election will have an increased focus on threats posed by potential foreign influence. The work will be organised in close cooperation with the appointed inter-governmental task force, especially DSIS and DDIS/CFCS.
>
> 6. The Government will offer all political parties eligible to be elected to Parliament counselling on the risk of foreign influence in relation to the upcoming parliamentary elections, including cyber-attacks, and on the options for countering such influence and attacks. The counselling will be offered through the national security authorities (DSIS and DDIS/CFSC).[62]

However, already in 2017 the Danish Government had announced increased collaboration between the Defense Department, Danish Security Intelligence Service, Danish Defense Intelligence Service, and Ministry of Justice.[63] At that time, the defense minister described cyberattacks as "the greatest threat against Denmark."[64]

C. Media Literacy Initiatives

The Open Society Institute, Sofia, published a Media Literacy Index 2018, ranking Denmark as the second most media-literate country in the EU.[65] A number of Danish media literacy projects are listed in a survey conducted by the EU in 2018.[66] They include both stakeholder and public authority initiatives, and most of them focus on critical thinking.[67] An example of a governmental media literacy program is the 2017 Danish Defense training of personnel stationed in Estonia, which included training in tactics on how to combat disinformation from Russian sources.[68] Another example is the 2015 report *Media Literacy in a Danish Context*.[69]

Increased media literacy among government employees was also one of the initiatives announced by the Danish government in 2018:

---

[62] Id.

[63] Andreas Baumann & Andreas Reinholt Hansen, *Danmark får ny kommandocentral mod misinformation* (Sept. 10, 2017), https://perma.cc/LG4U-23SQ.

[64] Id.

[65] European Policies Initiative, Open Society Institute Sofia, *Common Sense Wanted – Resilience to Post-truth and Its Predictors in the New Media Literacy Index 2018* at 3 (2018), https://perma.cc/98WR-CF2C.

[66] Council of Europe, *Mapping of Media Literacy Practices and Actions in EU-28* (2016), https://perma.cc/XLB6-EGJ4.

[67] Id. at 139.

[68] Andreas Nygaard Just & Simon Friis Degn, *Danske soldater skal beskyttes mod fake news fra Rusland*, DR (July 17, 2017), https://perma.cc/6H7Q-5944.

[69] Kulturstyrelsen, *Specialrapport Media Literacy i en dansk kontekst* (2015), https://perma.cc/79M8-HD99; see also *New Study: Media Literacy in Denmark*, Democracy and Citizenship in Digital Society (Dec. 18, 2015), https://perma.cc/9TXW-6MSB.

> 2. The Ministry of Foreign Affairs has launched a strengthened monitoring of disinformation in the media directed at Denmark and will – inspired by other Nordic countries – initiate training for communication officers from government authorities on the ongoing handling of disinformation.[70]

IV. Media Coordination

The government's action plan (the eleven initiatives mentioned above) include initiatives undertaken between media and the political parties.[71] Specifically, it provides as follows:

> 8. The Government will invite representatives from the media to a dialogue on possible models for cooperation on countering potential foreign attempts to influence the upcoming parliamentary elections. This will happen with full respect for the central principles of a free and independent press.
>
> 9. The Government will invite representatives from prevalent social media platforms to a dialogue on possible models for cooperation on countering potential foreign attempts to influence the upcoming parliamentary elections. This initiative will amongst other things be based on experiences from other countries.
>
> 10. The Government will invite media with public service obligations to a dialogue on models for cooperation on countering potential foreign attempts on influencing the upcoming parliamentary elections. One of the aims being to raise awareness about the threat amongst the population.[72]

Since the adoption of the initiatives Denmark has had a change in government, whether these initiatives will be carried over by the new government is currently unclear.

A. Industry Rules on Advertisement

The Danish media industry has launched a "labeling tool" whereby media publishers that are subject to the rules issued by the Danish Press Council mark their websites with a logo.[73] The Press Council has also issued guidelines for media actors.[74] Danish media is bound by the Responsible Media Act (Mediansvarsloven).[75] The Press Council reviews complaints made against the media for violating press guidelines.[76] Media actors (including media outlets using

[70] Press Release, Ministry of Foreign Affairs, supra note 57.

[71] Initiatives 8-10, *Styrket værn mod udenlandsk påvirkning af danske valg og demokratiet*, Udenrigsministeriet (Sept. 7, 2018), https://perma.cc/5AWA-DEBX.

[72] Press Release, Ministry of Foreign Affairs, supra note 57.

[73] *Vi tager ansvar for indholdet: Mærningsordning taget flot imod*, Danske Medier (Aug. 15, 2019), https://perma.cc/CA2N-QK4Q.

[74] *Hvorfor anmelde sig til Pressenævnet?*, Pressenævnet, https://perma.cc/A6TS-VHT3.

[75] Mediansvarsloven [Media Resposnibility Act] (LBK nr 914 af 11/08/2014), https://perma.cc/G25H-HLD2.

[76] *Verified Signatories of the IFCN Code of Principles*, IFCN Code of Principles, https://perma.cc/L2BB-CZ5Z.

Facebook sites) that have signed up are obliged to follow the decision by the Press Council and remove content, and/or pay monetary fines.[77]

B. Fact-Checking Website Tjekdet.dk

Danish media has one internationally verified fact-checking website that is a member of the International Fact Checking (IFCN) network; Tjekdet.dk.[78] During the 2019 Parliamentary elections, Tjekdet.dk worked together with Facebook to verify the accuracy of stories shared on Facebook.[79] Tjekdet.dk is owned and operated by Mandag Morgen, which describes itself as a combination of a media house and a think-tank.[80]

C. Misinformation During 2019 Election Campaign

Reports indicate that as many as half of all Danish voters were worried about fake news in connection with the Parliamentary election in 2019.[81] Moreover, almost one third were worried about foreign state interventions.[82] Also the Danish public media is concerned about the influence of foreign states on social media content. For example, Denmark blames Russia for the growing skepticism of 5G towers, as evidenced by social media.[83] Poul Madsen, the Executive Editor in Chief at EkstraBladet (a Danish tabloid), complained during the 2019 Parliamentary election that "[Danes] are bombarded with election messaging [*valgbudskab*] from all sides" on Facebook.[84]

---

[77] Id.

[78] *Om Tjekdet*, Tjekdet.dk, https://perma.cc/68ZX-YCPK; *Verified Signatories of the IFCN Code of Principles*, supra note 76.

[79] *Verified Signatories of the IFCN Code of Principles*, supra note 76; Ehsan Faizzad, *Facebook blev overrumplet af misinformation – her er løsningen*, Journalisten (May 8, 2019), https://perma.cc/8QLJ-6MKU.

[80] *Om Mandag Morgen*, Mandag Morgen, https://perma.cc/6U4G-DKPC.

[81] *Halvdelen af vælgerne frygter fake news i forbindelse med folketingsvalget*, KMD (May 3, 2019), https://perma.cc/3GPG-8KL3.

[82] Id.

[83] Fredrik Hugo Ledegaard et al., *5G-modstandere spreder russisk misinformation i Danmark*, DR (May 31, 2019), https://perma.cc/UTE6-SZ6B.

[84] Poul Madsen, *Facebook er Danmarks Største Central for Misinformation*, EkstraBladet (Feb. 10, 2019), https://perma.cc/5X2W-C7S9.

Egypt

George Sadek
Foreign Law Specialist

SUMMARY The Egyptian government has passed three domestic laws to regulate the distribution of information and ensure its accuracy in both print and online media, including on social networks. Those laws include Law No. 175 of 2018 on Anti-Cybercrime, Law No. 180 of 2018 on Regulating the Press and Media, and Law No. 58 of 1937 and its amendments on the Penal Code.

The Egyptian government is fighting what is considered misinformation by suspending websites and social media accounts, trying to establish a local social media platform to replace Facebook, creating a hotline to report false news circulating on social media outlets, imposing fines on newspapers posting news deemed false by the Egyptian authorities, and arresting and detaining individuals whom the government accuses of spreading false news through social media platforms.

I. Background

According to news reports, Egypt has the highest number of Facebook users in the Arab world with 34.5 million Egyptians having active accounts, which represents 23% of all Arab Facebook users.[1]

In 2018, President of Egypt Abdu-Al-Fatah al-Sisi claimed that the Egyptian government had identified around 21,000 rumors that were circulated on social media over a three-month period that year.[2] In 2017, the Communication and Information Technology Committee in the Egyptian Parliament revealed that 53,000 false rumors had spread in Egypt in just sixty days. The Committee announced that most of this false news had originated and circulated on social media platforms.[3] In an effort to combat the dissemination of false news, the Cabinet issues statements refuting false information circulated in the media or via online social networks.[4]

In June 2019, the undersecretary of the General Directorate of Information and Relations at the Egyptian Interior Ministry declared that there are around 4 to 6 million pages allegedly circulating misinformation on social media accounts targeting Egyptians.[5]

---

[1] *Egypt to Establish 'Egyptian Facebook': Minister*, Al-Ahram (Mar. 12, 2018), https://perma.cc/V623-AGGA.

[2] Samy Magdy, *Egypt Says It Fights Fake News, Critics See New Crackdown*, Associated Press (Sept. 17, 2018), https://perma.cc/REV4-GZKL.

[3] Amina Khairy, Op-Ed., *Trapped in a Sea of Rumors*, Al-Ahram Weekly (Aug. 1, 2018), https://perma.cc/8R75-VVRN.

[4] Magdy, supra note 2.

[5] *Egypt Reported to Have 4-6m Fake News Pages*, Arab News (June 16, 2019), https://perma.cc/5KG9-RZ56.

II. Current Legislation

The Egyptian government has passed four domestic laws to regulate the distribution of information and ensure its accuracy in both print and online media, including on social networks. Those laws include Law No. 175 of 2018 on Anti-Cybercrime, [6] Law No. 180 of 2018 on Regulating the Press and Media,[7] and Law No. 58 of 1937 and its amendments on the Penal Code.[8] In 2014, the Egyptian Parliament also passed Law No. 45 of 2014 on the practice of political rights regulating the content of electoral campaigns.[9]

A. Law 180 of 2018 Regulating the Press and Media

Law No. 180 of 2018 stipulates that press institutions, media outlets, and news websites must not broadcast or publish any information violating the principles cited under the Constitution, granting the Supreme Media Council the authority to ban or suspend the distribution, broadcast, or operation of any publications, newspapers, media outlets, or advertising materials containing information deemed to threaten national security; disturb the public peace; or promote discrimination, violence, racism, hatred, or intolerance.[10]

The Law authorizes the Supreme Media Council to suspend or block any personal website, blog, or social media account that has a high number of followers—exceeding 5,000—if it publishes fake news advocating and inciting the violation of a specific law or promoting violence or hatred.[11] The Council was created by Law No. 92 of 2016.[12] It is composed of a Chairman who is selected by the President of the Republic and twelve members representing the Parliament, Administrative Court, Journalists Association, National Authority to Regulate Communication, Anti-Monopoly Authority, Supreme Council of Universities, and media experts.[13] The Council reports to the President of the Republic and the Parliament.[14] The role of the Council is to regulate and supervise media outlets in all of their forms: print, broadcast, and electronic.[15]

Law No. 180 of 2018 also prohibits news outlets from posting information in print or online concerning a specific court case if such information will negatively affect the defendant in the case or the trial proceedings.[16] Media outlets must rectify any false information that was posted

[6] Law No. 175 of 2018, Al-Jaridah Al-Rasmiyah, vol. 32 (bis)(c), 14 Aug. 2018.

[7] Law No. 180 of 2018, Al-Jaridah Al-Rasmiyah, vol. 34 (bis)(h), 27 Aug. 2018.

[8] Penal Code, Law No. 58 of 1937, as amended by Law No. 95 of 2003, vol. 25, Al-Jaridah Al-Rasmiyah, 19 June 2003.

[9] Law 45 of 2014, Al-Jaridah Al-Rasmiyah, vol. 23(bis) (5 June 2014), https://perma.cc/DD23-L3VM.

[10] Law 180 of 2018, art. 4.

[11] Id. art. 19.

[12] Law No. 92 of 2016, Al-Jaridah Al-Rasmiyah, vol. 52 bis, 24 Dec. 2016.

[13] Id. art. 6.

[14] Id. art. 23.

[15] Id. art. 4.

[16] Law 180 of 2018, art. 21.

on their websites without any financial compensation. This is meant to prevent media outlets from demanding payment as a condition for withdrawing or correcting false information they publish. Such rectification must take place within three days from the date of being notified that the information posted was false.[17]

Directors of media outlets or website administrators who violate the provisions on posting case-related information or fail to rectify false information are punishable with a fine of between 50,000 and 100,000 Egyptian pounds (about US$2,855–$5,711).[18]

B. Law No. 175 of 2018 on Anti-Cybercrime

Law No. 175 of 2018 grants the investigating authority the power to block or suspend Egyptian-based or foreign websites featuring content that is deemed threatening to national security or the national economy.[19]

Additionally, any individual who hacks a website in order to alter the information posted on such website or redistributes such information after altering it is punishable with a term of imprisonment of not less than two years, a fine of between 100,000 and 200,000 Egyptian pounds (about US$5,700–$11,400), or both.[20] Individuals who hack a government website in order to erase or modify information posted on the website, or redistribute the information after modifying it, are punishable with a term of imprisonment and a fine of between 1 million and 5 million Egyptian pounds (about US$57,000–$285,000).[21]

The public prosecutor is authorized to impose a travel ban on individuals suspected of committing any act considered a crime under Law 175.[22]

C. Penal Code, Law No. 58 of 1937, and Its Amendments

The Penal Code states that whoever deliberately spreads false information or rumors abroad about the internal conditions of the country that might weaken the country's financial credibility or harm the country's national interests is punishable by six months' to five years' imprisonment and a fine.[23]

D. Law No. 45 of 2014

Candidates are prohibited from using any negative ads. Law No. 45 of 2014, regulating the practice of political rights, prohibits candidates from using any religious slogans, calls for

[17] Id. art. 22.

[18] Id. art. 101.

[19] Law 175 of 2018, art. 7.

[20] Id. art. 14, para. 2.

[21] Id. art. 20, para. 3.

[22] Id. art. 9.

[23] Penal Code art. 80(d).

discrimination, ads attacking other candidates, or electoral propaganda threating national unity of the Egyptian people in their electoral campaigns.[24]

III. Law Enforcement

The Egyptian authorities are enforcing anti-misinformation legislation by imposing fines on newspapers posting news online that the authorities deem false, and arresting and detaining individuals whom the government accuses of spreading false news through social media platforms.

In September 2018, the Associated Press reported that the Egyptian authorities had suspended or blocked five hundred websites that were suspected by the authorities of distributing false information.[25] Those blocked websites included a number of news sites such as *Huffington Post Arabic*, the financial newspaper *Al-Borsa*, and the entire online publishing platforms of the *Medium* and *Mada Masr*. The Egyptian government also blocked websites related to human rights organizations such as the Association for Freedom of Thought and Expression, Human Rights Watch, and Reporters Without Borders. Similarly, websites belonging to political movements like the April 6 Movement and the Muslim Brotherhood are also blocked.[26]

Furthermore, the Egyptian authorities have imposed fines on some newspapers accusing them of disseminating false information online. For instance, in April 2018, State Security Prosecution summoned the editor-in-chief of the newspaper *Al-Masry Al-Youm* and seven correspondents, accusing them of distributing false information. In another example, Adel Sabri, Editor-in-Chief of the *Masr El-Arabiya* website was detained and charged with the dissemination of false news. The website was also fined 50,000 Egyptian pounds (about US$2,855) by the Supreme Council for Media Regulation for disseminating false information.[27] Similarly, according to a report issued by the Tahrir Institute for Middle East Policy in 2019, the Egyptian authorities imposed a fine on the weekly newspaper *al-Mashed* and blocked the newspaper's website for six months after it published an article about security personnel extorting business owners in Cairo. The Supreme Media Council has also accused the newspaper of disseminating false news and invading the privacy of an Egyptian actress.[28]

Finally, the Egyptian authorities have detained some individuals, accusing them of the dissemination of false news on Facebook and Twitter. Political and human rights activists such as Abdel Khalek Farouk, Amal Fathi, Ibrahim Khateib, Hazem Abdel-Azim, and Shady Harb were all charged with using social media to spread false information. These individuals have

[24] Law 45 of 2014, art. 31.

[25] Magdy, supra note 2.

[26] *Freedom on the Net 2018: Egypt,* Freedom House (2018), https://perma.cc/UQ7Y-YCFY.

[27] *The Quarterly Report on the State of Freedom of Expression in Egypt, 2nd Quarter (Apr.-June 2018)*, Freedom of Thought and Expression (Oct. 15, 2018), https://perma.cc/LU79-VK8M.

[28] *TIMEP Brief: Press Freedom in Egypt*, The Tahrir Institute for Middle East Policy (May 24, 2019), https://perma.cc/P3ZD-V5S3.

argued that they were just expressing their opinion online and that the government falsely accused them of disseminating false information.[29]

IV. Other Government Actions

The Egyptian government is fighting what is considered online misinformation by suspending websites and accounts on social media, trying to establish a local social media platform, and creating a hotline to report false news circulating on social media outlets.

In March 2018, Telecommunication and Information Technology Minister Yasser El-Kady announced that, in its effort to eliminate any misinformation currently circulating through social media outlets and combat extremist ideology, the Egyptian government was taking effective steps towards creating an Egyptian local version of Facebook.[30]

In an extra measure to prevent the dissemination of false news, the Egyptian Public Prosecutor has announced the creation of a new hotline for citizens to file complaints against false news posted by media outlets or by individuals on social media networks.[31]

Ali Abaza, the Director of the Interior Ministry's Cyber Crimes Department, has also declared that more than 1,000 Facebook pages were closed in 2016 alone for inciting violence against police and army officers, and calling for protests.[32]

V. Media Coordination

Based on a report issued in 2018 by Freedom House, the Egyptian authorities may have a role in removing online content that is deemed false by the government. For instance, in October 2017, the newspaper *Al-Masry Al-Youm* argued that an anonymous hacker had removed an article criticizing the president from their website. Likewise, in May 2018, the State Information Service at the Ministry of Foreign Affairs ordered *Russia Today's* Arabic website to remove an online poll that it had posted on the disputed territories of Halayeb and Shalateen on the border between Egypt and Sudan.[33]

[29] Salma Islam, *In 'Fake News' Crackdown, Egypt Is a World Leader on Jailing Journalists, Bloggers and Social Media Users*, Los Angeles Times (Dec. 18, 2018), https://perma.cc/8ZH4-AZ9E.

[30] Magdy, supra note 2.

[31] Jehad El-Sayed, *How Can Egypt Combat Fake News?*, Egypt Today (Mar. 15, 2018), https://perma.cc/644Y-R5SJ.

[32] *1,045 Facebook Pages Were Closed in 2016 for Inciting Violence: Egypt Interior Ministry*, Ahram Online (Dec. 24, 2016), https://perma.cc/3KE7-UE8J.

[33] *Freedom on the Net 2018: Egypt,* supra note 26.

European Union

Elin Hofverberg
Foreign Law Specialist

SUMMARY The European Union (EU) recognizes and protects the right to freedom of speech, including on the internet. It has not adopted any regulation on the use of internet platforms for political advertising. Therefore, online political advertisements are governed by the laws of individual member countries. However, the EU has taken a number of initiatives to counter disinformation online. The European Commission has developed a non-binding ten-item action plan for member states dealing with disinformation and has also developed a Code of Practice on Disinformation for social media platforms to use in connection with, among other things, political advertisements. The Code specifically requires that signatories of ensure that political advertisements are distinguishable from editorial content. So far, thirteen social medial platforms and trade associations have signed the Code. Other EU initiatives include funding projects targeting misinformation, creating a misinformation website, and calling on member states to increase the transparency of online advertisements.

I. Background

A. Dissemination of Disinformation in the EU

The European Commission recognizes disinformation as a "major challenge for Europe."[1] It has declared that "[d]emocracy in the European Union rests on the existence of free and independent media."[2] In 2016, a survey found that 57% of EU citizens used social media or search engines as the main source of news.[3] According to the European Commission, 80% of Europeans have encountered information that they perceived as "false or misleading several times a month or more."[4]

B. Principles of Free Speech

Freedom of speech is recognized as an international human right by the EU and is guaranteed through the Charter of Fundamental Rights of the European Union, which states:

[1] European Commission, *Tackling Online Disinformation: A European Approach* 1 (COM(2018) 236 final, Apr. 26, 2018), https://perma.cc/W3K9-PSXJ.

[2] Id.

[3] Id. at 2. See also European Union, *Flash Eurobarometer 437 Report: Internet Users' Preferences for Accessing Content Online* (Mar. 2016), https://perma.cc/GY58-8VQ7.

[4] *Tackling Online Disinformation: A European Approach*, supra note 1, at 3.

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
>
> 2. The freedom and pluralism of the media shall be respected.[5]

Freedom of speech is also recognized in the Treaty on the European Union.[6] In addition, all EU member states are members of the European Convention on Human Rights, and all EU member countries protect freedom of speech in their constitutions.[7] The European Court of Human Rights has established that freedom of expression includes a right to expressions of speech that "offend, shock, or disturb."[8]

II. Legislation

There is no EU-wide legislation that deals with political advertisements, which means that member countries are responsible for these laws. However, the Audiovisual Media Services Directive deals with media literacy.[9] It defines media literacy as "skills, knowledge and understanding that allow citizens to use media effectively and safely."[10] It adds that,

> [i]n order to enable citizens to access information and to use, critically assess and create media content responsibly and safely, citizens need to possess advanced media literacy skills. Media literacy should not be limited to learning about tools and technologies, but should aim to equip citizens with the critical thinking skills required to exercise judgment, analyse complex realities and recognise the difference between opinion and fact. It is therefore necessary that both media service providers and video-sharing platforms providers, in cooperation with all relevant stakeholders, promote the development of media literacy in all sections of society, for citizens of all ages, and for all media and that progress in that regard is followed closely.[11]

A. Commission Recommendation on Online Transparency

On September 12, 2018, the European Commission issued a recommendation ahead of the 2019 European Parliament elections that, among other things, addressed online transparency with

---

[5] Charter of the Fundamental Rights of the European Union, 2000 O.J. (C 364) art. 11, https://perma.cc/C5R8-8D2G.

[6] Treaty on the European Union, 2012 O.J. (C326) art. 6(1), https://perma.cc/AJK9-VS36.

[7] European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms (1950)), https://perma.cc/6F24-P2RA; *Chart of Signatures and Ratifications of Treaty 005 Convention for the Protection of Human Rights and Fundamental Freedoms Status as of 26/08/2019*, Council of Europe (Aug. 26, 2019), https://perma.cc/KK67-7ZJL.

[8] *Handyside v. United Kingdom*, App. No. 5493/72 (7 December 1976), § 49, https://perma.cc/XX43-UF2K.

[9] Audiovisual Media Service Directive, 2010 O.J. (L95, 1) art. 33a, https://perma.cc/RLW2-Q868, inserted by Directive 2018/1808 amending the Audiovisual Media Service Directive, 2018 O.J. (L 303, 69) art. 1, https://perma.cc/8LL3-Y8QM.

[10] Id. Preamble para. 59.

[11] Id.

regard to political advertisements and political campaigns.[12] It is not binding on the EU member states but calls on them to "encourage" online transparency "by promoting active disclosure of who is behind paid online political advertisements and communications during electoral campaigns, while fully respecting freedom of expression."[13]

B. Action Plan against Disinformation

In 2018, the EU adopted an action plan against disinformation.[14] The plan sets out a total of ten actions, ranging from collaboration between the High Representative of the Union for Foreign Affairs and Security Policy (similar to a foreign minister) and the member states on how to "detect, analyse and expose disinformation activities,"[15] to continued close monitoring of the implementation of the Code of Practice on Disinformation, discussed below.[16] Media literacy is also an integral part of the Action Plan, and efforts to increase media literacy among citizens of the European Union include a Media Literacy Week (March 2019)[17] and public training for "media and public opinion shapers in the Union.[18]"

III. Non-Legislative Actions

A. Calls for Transparency in Political Advertising

The European Commission has repeatedly called for EU member countries to enhance the transparency of political campaigns and advertising. For example, ahead of the 2019 EU Parliament elections, it called on national political parties to ensure free and fair elections by "ensur[ing] transparency of political advertising, [by being] ready to face cyberattacks and [by] respect[ing] European data protection rules during the campaign."[19] The Commission has also

[12] Commission Recommendation on Election Cooperation Networks, Online Transparency, Protection against Cybersecurity Incidents and Fighting Disinformation Campaigns in the Context of Elections to the European Parliament (C(2018) 5949 final, Sept. 12, 2018), https://perma.cc/ZV84-D2CS.

[13] Id. para. 16.

[14] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Action Plan against Disinformation* (JOIN(2018) 36 final, Dec. 5, 2018), https://perma.cc/J8Z2-XZJB. In 2015, the European Council called upon the High Representative to develop an action plan to address Russia's ongoing disinformation campaigns: European Council, EUCO 11/15, 5 (Mar. 20, 2015), https://perma.cc/NP8R-GLJC.

[15] *Action Plan against Disinformation*, supra note 14, at 6.

[16] Id. at 9 & 11. See also *A Europe that Protects: The EU Steps Up Action Against Disinformation*, European Commission (Dec. 5, 2018), https://perma.cc/FVN5-U649; Press Release, European Commission, A Europe that Protects: The EU Steps Up Action Against Disinformation (Dec. 5, 2018), https://perma.cc/8Y4R-2HZ4.

[17] Press Release, European Commission, Launch of the European Media Literacy Week – 18 to 22 March 2019, https://perma.cc/5HR8-FHRD.

[18] *Action Plan against Disinformation,* supra note 14, at 11.

[19] Press Release, European Commission, European Commission Calls on National Political Parties to Join Efforts to Ensure Free and Fair Elections in Europe (Mar. 15, 2019) https://perma.cc/H8WB-F933.

published an independent report on fake news and online disinformation.[20] The purpose of the report is to provide member states with options on how to counter the online spread of disinformation and to "help develop a comprehensive EU Strategy for tackling disinformation."[21]

In addition, a number of high-profile EU officials have called for transparency in political advertising. For example, in his 2018 State of the Union address, then-President of the European Commission, Jean-Claude Junker, announced a "set of concrete measures, including greater transparency in online political advertisements and the possibility to impose sanctions for the illegal use of personal data in order to deliberately influence the outcome of the European elections."[22] The European Commission also recommended that

> European and national political parties, foundations and campaign organisations should make available information on their expenditure on online advertising campaigns, by disclosing which party or political support group is behind online political advertisements as well as by publishing information on targeting criteria used to disseminate information to citizens. Where these principles are not followed, Member States should apply national sanctions.[23]

B. East StratCom Task Force and Rapid Alert System

The East StratCom Task Force was created within the European External Action Service with the purpose of "address[ing] Russia's ongoing disinformation campaigns."[24]

The East StratCom Task Force has set up an *EU v Disinformation* webpage, which functions as an EU-wide rapid alert system and is meant to "facilitate the sharing of insights related to disinformation campaigns and coordinate responses."[25] The system is based on open-source information and also draws expertise from "academia, fact-checkers, online platforms and international partners."[26] The website offers access to a database of disinformation cases.[27] Information on the web page states that,

> [t]o date, the Task Force has catalogued, analysed and raised awareness of over 4,500 examples of pro-Kremlin disinformation, and significantly improved understanding of the tools, techniques and intentions of disinformation by Russian sources. In close cooperation

[20] European Commission, *A Multi-dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation* 2 (2018), https://perma.cc/V29P-B7TC.

[21] Id.

[22] Press Release, European Commission, State of the Union 2018: European Commission Proposes Measures for Securing Free and Fair European Elections (Sept. 12, 2018), https://perma.cc/3EXY-3XHU.

[23] Id.

[24] *Questions and Answers about the East StratCom Task Force*, European Union External Action (May 12, 2018), https://perma.cc/Z3F6-TQVF; *About the European External Action Service (EEAS)*, European Union External (Jan. 3, 2016), https://perma.cc/J5YY-VAK5.

[25] *About*, EU v Disinfo, https://perma.cc/DKL5-ZTMH.

[26] Id.

[27] *Disinformation Cases*, EU vs Disinfo, https://perma.cc/9GBU-VMCQ.

with European Commission services, it has also substantially improved the effectiveness of EU communications in the Eastern Neighbourhood.[28]

C. Fact-checking Network

The EU is funding a joint EU-wide network for fact-checkers.[29] In total, €2.5 million (approximately US$2.8 million) has been budgeted for this purpose.[30] In addition, as part of a global media cooperation effort, the International Fact-Checking Network (IFCN) has developed a EU-specific fact-checking site, FactCheckEU.info,[31] "bringing together the European signatories of IFCN's Code of Principles to counter misinformation in the European Union at a continental scale ahead of the European Parliament elections of May 2019."[32]

D. Co-funding of Projects in the Field of Media Freedom and Pluralism

The European Commission co-funds (together with the European Parliament) "independent projects in the field of media freedom and pluralism. These projects, among other actions, monitor risks to media pluralism across Europe, map violations to media freedom, fund cross-border investigative journalism and support journalists under threat."[33] According to the European Commission, as of January 2019, approximately €40 million (approximately US$44 million) has been invested in these types of projects.[34] In addition, the European Commission has proposed a budget of €61 million (approximately US$68 million) for the period from 2021 to 2027 towards the Creative Europe program, which supports the audiovisual sectors of Europe.[35]

IV. Media Coordination

A. Requirements of the Code of Practice on Disinformation

In 2018, the European Commission developed the *EU Code of Practice on Disinformation*, which applies to social media platforms.[36] The EU Code of Practice was signed by Facebook, Google,

---

[28] *Countering Disinformation,* European Union External Action, https://perma.cc/ZLR9-48RT.

[29] *Questions and Answers – Code of Practice against Disinformation: Commission Calls on Signatories to Intensify their Efforts*, European Commission (Jan. 29, 2019), https://perma.cc/P6ZR-G7AQ.

[30] Id.

[31] FactCheckEU.info, https://perma.cc/5BEY-UA4U.

[32] *About Us*, FactCheckEU.info, https://perma.cc/GV5T-CFJE.

[33] *Questions and Answers – Code of Practice against Disinformation: Commission Calls on Signatories to Intensify their Efforts,* supra note 29.

[34] Id.

[35] Id.

[36] *EU Code of Practice on Disinformation* (2018), https://perma.cc/T9CX-9755; *Code of Practice on Disinformation*, European Commission (Sept. 26, 2018), https://perma.cc/SE58-9Z3P. See also Jenny Gesley, *European Union: Commission Proposes EU-Wide Code of Practice to Combat Fake News Online*, Global Legal Monitor (May 11, 2018), https://perma.cc/3QKF-6N7M.

Twitter, and Mozilla, as well as advertising trade associations, on October 16, 2018.[37] It has since been signed by a total of thirteen signatories.[38] The purpose of the Code is to "identify the actions that Signatories could put in place in order to address the challenges related to 'Disinformation'."[39]

The Code of Practice specifically mentions political advertising.[40] Among other things, the Code states that "[t]he Signatories of the Code of Practice recognize the importance of efforts to"

> . . .
>
> (iii) Ensure transparency about political and issue-based advertising, also with a view to enabling users to understand why they have been targeted by a given advertisement.
>
> . . .
> (viii) Ensure transparency with a view to enabling users to understand why they have been targeted by a given political or issue-based advertisement, also through indicators of the trustworthiness of content sources, media ownership and/or verified identity.[41]

Compliance with the Code further requires that advertisements "should be clearly distinguishable from editorial content."[42] Signatories also have a duty to "use reasonable efforts towards devising approaches to publicly disclose 'issue-based advertising'."[43]

B. Social Media Platform Responses to the Code

Social media platforms have responded to the Code in a variety of ways. For instance, Google has changed its policies and now includes policies and information that specifically apply to the EU:

> In the EU, election ads include ads that feature:
>
> - a political party, a current elected officeholder, or candidate for the EU Parliament;
> - a political party, a current officeholder, or candidate for an elected national office within an EU member state. Examples include members of a national parliament and presidents that are directly elected.
>
> Note that election ads don't include ads for products or services, including promotional political merchandise like t-shirts, or ads run by news organizations to promote their

[37] Press Release, European Commission, A Europe that Protects: The EU Steps Up Action against Disinformation, supra note 16.

[38] *Roadmaps to Implement the Code of Practice on Disinformation*, European Commission (Oct. 16, 2018), https://perma.cc/9C65-JCGQ.

[39] *EU Code of Practice on Disinformation*, supra note 36, § I.

[40] Id.; *Code of Practice on Disinformation*, supra note 36.

[41] *EU Code of Practice on Disinformation*, supra note 36, § I.

[42] Id. § II.B para. 2.

[43] Id. § II.B para. 4.

> coverage of political parties, EU election campaigns, candidates, or current elected officeholders.[44]

Google's policies provide that Election ads in the EU may run only if the advertiser is verified by Google.[45]

Twitter has also published guidelines specifically targeting political content published by businesses operating in the EU:

> Political Content includes political campaigning and issue advocacy advertising.
>
> - Political campaigning ads are permitted in the European Union (EU) except in the following countries: Cyprus, Latvia, Lithuania, France, Hungary, and Portugal.
> - Political campaigning ads for EU Parliamentary Elections ONLY must meet additional eligibility requirements and apply for certification.
> - Issue advocacy ads are permitted without restriction except in France.
>
> Political campaigning ads may only be promoted via the use of Promoted Tweets and In-Stream Video Ads; no other Twitter advertising products can be used at this time.
>
> **Political Campaigning**
>
> Policy
>
> EU Parliamentary elections only.
>
> Political campaigning ads refers to ads that fall under any of the criteria listed below:
>
> - Ads purchased by a European or national political party,
> - Ads purchased by a candidate registered with their corresponding national electoral authority, or
> - Ads that advocate for or against a clearly identified candidate or party for European elections.
>
> Requirements
>
> Political campaigning advertisers must go through Twitter's certification process* and meet the following requirements:
>
> - Profile photo, header photo, and website must be consistent with the handle's online presence.
> - Bio must include a website that provides valid contact info. Political parties and European Parliament candidates should indicate their European political party affiliation.
> - If handle name is not related to the certified entity, the bio must include the following disclaimer: "Owned by [certified entity name]".

[44] *Advertising Policies Help - Political Content*, Google, https://perma.cc/JG34-XXPM.

[45] Id.

*Political advertisers will be required to provide additional information for Twitter to verify identity and location. Such information will be used for this sole purpose only.

Restrictions

- Political campaigning advertisers must comply with applicable laws regarding disclosure and content requirements, eligibility restrictions, spending limits, reporting requirements, and blackout dates for the countries where they advertise.
- Political campaigning advertisers can only use currencies from EU member countries where political campaigning is permitted.

Once certified, political campaigning advertisers will be prompted to use "Paid for by" disclaimers. Disclaimers must not be misleading and match website or certification application.[46]

C. EU Response to Implementation of the Code

In January 2019, the European Commission and the High Representative made calls for increased efforts by the signatories (Facebook, Google, Twitter, Mozilla, and advertising trade associations).[47] The calls were a response to the mandated annual reports on measures undertaken by the social media platforms, as required under the Code.[48] The European Commission noted that although the Code is voluntary in nature, by signing on, the signatories "have committed to taking precise, measurable and concrete measures to fight online disinformation."[49] The European Commission also noted that it appeared that social media platforms only made consumer empowerment tools available to "a limited number of Member States."[50] For example, Facebook's "context" button was only available in some EU member states.[51] The goal of the Code is that consumer's ultimately will be able to "easily identify and report information they receive as disinformation, and platforms will take action to reduce the visibility and dissemination of this content."[52]

[46] *Political Content in the European Union*, Twitter, https://perma.cc/2WZS-GGTG.

[47] *Questions and Answers – Code of Practice against Disinformation: Commission Calls on Signatories to Intensify their Efforts*, European Commission (Jan. 29, 2019), https://perma.cc/P6ZR-G7AQ

[48] *First Results of the EU Code of Practice against Disinformation*, European Commission (Jan. 29, 2019), https://perma.cc/R7XL-PSRS. See also *Code of Practice against Disinformation*, European Commission (Jan. 29, 2019), https://perma.cc/PNW9-UVP5.

[49] *First Results of the EU Code of Practice against Disinformation*, supra note 48.

[50] Id.

[51] Id.

[52] Id.

France

Nicolas Boring
Foreign Law Specialist

SUMMARY Fake news and political advertising are two areas where speech is highly regulated in France. The publication or dissemination of fabricated information falsely attributed to a third party is illegal under French defamation laws. Paid political advertising in newspapers, on the radio, on television, or online is strictly forbidden for at least six months before an election. Additionally, there is a "period of silence" on election day and the day before, during which all campaigning must stop. This means that any political advertising, even unpaid advertising, is illegal during that period. In addition to these rules, a new law was adopted in December 2018 that aims to prevent the dissemination of fake news, particularly during electoral campaigns. This new law imposes transparency requirements for online advertising and creates a new legal weapon for combating the dissemination of fake news during an election period. It also gives more authority to France's main broadcasting regulatory agency to act against the propagation of false information, particularly when it originates from a foreign government. In addition to legislation, the French government has taken actions against the spread of fake information. During the 2017 presidential elections, government agencies were proactive in helping the candidates' campaigns counter hacking and disinformation attempts. The government is adding media literacy to public school curriculums, and the French broadcasting regulatory agency has issued recommendations for online platform operators to fight against the spread of fake news. Partially in response to French legislation, the main online platform operators have taken steps to increase transparency and counter the spread of misinformation on social media.

I. Introduction

Freedom of expression is considered an "essential freedom" in France.[1] It is protected by the French Constitution, which incorporates the Declaration of Human and Civic Rights of 1789.[2] Articles 10 and 11 of the Declaration protect freedoms of opinion and expression, describing the "free communication of ideas and of opinions" as "one of the most precious rights of man."[3] Similarly, the European Convention on Human Rights, by which France is bound, provides that "Everyone has the right to freedom of expression," including "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[4]

[1] Xavier Dupré de Boulois, *Droit des libertés fondamentales* 360 (2018).

[2] Const. du 4 octobre 1958, Preambule (2019), https://perma.cc/95S6-F4KX.

[3] Déclaration des Droits de l'Homme et du Citoyen de 1789, art. 11, https://perma.cc/G3K5-CBGQ.

[4] European Convention on Human Rights, art. 10 (2010), https://perma.cc/BFR2-WU6M.

Freedom of speech was never intended to be absolute, however. In contrast to the First Amendment of the US Constitution, the 1789 Declaration of Human and Civic Rights provides limits to freedom of expression in its very definition. Article 10 declares that "No one may be disturbed on account of his opinions, even religious ones, as long as the manifestation of such opinions does not interfere with the established Law and Order."[5] Article 11 provides that "[a]ny citizen may therefore speak, write and publish freely, except what is tantamount to the abuse of this liberty in the cases determined by Law."[6] Similarly, the European Convention on Human Rights declares that freedom of speech, "since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society . . . ."[7]

The subject of this report represents the intersection of two areas where freedom of speech is strictly regulated in France: "fake news," including defamation, on the one hand, and advertising, including political advertising, on the other. A number of legal provisions have long been in place, but the advent of the internet, and particularly social media, has created challenges that spurred the recent adoption of new legislation.

II. Current and Pending Legislation

A. General Limits on Disseminating Fake News and Defamatory Speech

"Fake news" is one of the areas where freedom of speech has long been strictly regulated in France. Indeed, French law prohibits the bad-faith "publication, dissemination or reproduction, by any means, of fake news, [and] items that were made-up, falsified, or untruthfully attributed to third parties," when those acts might disturb public peace.[8] Such acts are punishable by a fine of €45,000 (approximately US$49,900).[9] Additionally, defamation and public insults are also prohibited, and are punishable by fines of €12,000 Euros (about US$13,300), or €45,000 if the defamation or insult was based on the victim's ethnicity, nationality, race, religion, sex, sexual orientation, gender identification, or disability.[10]

B. Limits on Paid Political Advertising

Political advertising is another area where speech is highly regulated in France. Indeed, from the first day of the sixth month preceding an election until the end of that election, paid political advertising in newspapers, on the radio, or on television, is strictly forbidden.[11] The legislation

[5] Déclaration des Droits de l'Homme et du Citoyen de 1789, art. 10.

[6] Id. art. 11.

[7] European Convention on Human Rights, supra note 4, art. 10.

[8] Loi du 29 juillet 1881 sur la liberté de la presse (current version), art. 27, https://perma.cc/WV8K-YNF9.

[9] Id.

[10] Id. arts. 29–35.

[11] Code électoral, art. L52-1, https://perma.cc/MKZ2-LYQH.

that instituted this prohibition was adopted in 1990,[12] but the rise of the internet opened a new medium for political advertising that was unforeseen by its drafters. Indeed, the internet is considered a medium separate from the press and "audiovisual" media (which, in French, essentially refers to radio and television) that are covered by the 1990 legislation, and it therefore opened an important loophole to the prohibition on pre-election advertising.[13]

To close this loophole, a 2011 law extended all existing restrictions on political advertising to the internet.[14] The 1990 law prohibiting pre-election paid political advertising therefore now applies to the internet as well.[15] Thus, while it is perfectly legal for a political party, candidate, or campaign to have a website, a Facebook page, a Twitter account, or any similar internet presence, it is illegal to pay for political advertising during the period that runs from the first day of the sixth month before an election, up to the end of the election. For example, the first round of the last French presidential election took place on April 23, 2017, and the second round took place on May 7, 2017.[16] From October 1, 2016, until the closing of the last polling station on May 7, 2017, the candidates and their campaigns were prohibited from buying ads on the internet.[17] This includes not only banner ads, but also other advertising techniques such as paid referencing, sponsored links, or the purchase of key words on search engines.[18]

The penalty for breaching the pre-election prohibition on paid political advertising is a fine of up to €75,000 (approximately US$84,000).[19]

C. Pre-Election Period of Silence

French law prohibits any campaigning during election day and the day preceding it.[20] This period is referred to as the *période de réserve* (period of silence).[21] Political advertising of any type—not

[12] Loi n° 90-55 du 15 janvier 1990 relative à la limitation des dépenses électorales et à la clarification du financement des activités politiques (Jan. 15, 1990) (in French), https://perma.cc/KJU4-RG9R.

[13] Jérome Grand d'Esnon & Philippe Blanchetier, *Campagnes électorales* 106 (2007).

[14] Loi n° 2011-412 du 14 avril 2011 portant simplification de dispositions du code électoral et relative à la transparence financière de la vie politique, art. 2 (Apr. 14, 2011) (in French), https://perma.cc/JN5A-QGJZ.

[15] C. électoral, arts. L48-1 to L52-1.

[16] Stéphanie Alexandre, *Elections présidentielles et législatives: les dates de 2017*, Le Figaro (May 20, 2017), https://perma.cc/H6J8-PEYS.

[17] Conseil constitutionnel, *Quelles sont les obligations d'un candidat concernant la campagne sur Internet?* (undated), https://perma.cc/5M3J-V93Q.

[18] Julien Lausson, *Un candidat peut-il faire campagne aux législatives avec Facebook?*, Numérama (May 29, 2017), https://perma.cc/JC3T-9MKB; *Communication et campagne électorale: un cadre contraint*, Vie-publique.fr (French government website) (Nov. 19, 2013), https://perma.cc/R8NM-FGBQ.

[19] C. électoral, art. L90-1.

[20] C. électoral, arts. L48-2, L49, L49-1.

[21] Charlotte Belaich, *«Période de réserve»: de quoi peut-on parler ce week-end?*, Libération (Apr. 21, 2017), https://perma.cc/65QT-SJ7W.

just paid advertising—is prohibited during this period.[22] Furthermore, this prohibition applies not only to the candidates and their campaigns, but also to journalists, commentators, and any person or institution that could be seen as a direct or indirect proxy.[23] While the print media is allowed to publish political commentary during the period of silence, other media (radio, television, and internet-based) in France must refrain from doing so.[24]

Engaging in political advertising during the period of silence is punishable by a fine of up to €3,750 (approximately US$4,200).[25]

In theory, at least, private individuals are also supposed to abide by the period of silence. Indeed, the Conseil constitutionnel (Constitutional Council), which supervises national elections in France, warned that private citizens are not exempted from respecting the period of silence, and that "it is therefore preferable to abstain from any advocacy[26] activity on the day before and the day of the elections."[27] In practice, however, this rule appears difficult to enforce against regular, private individuals.[28]

D. New Law Against Fake News

On December 22, 2018, President Emmanuel Macron signed a new law against the dissemination of false information.[29] This legislation was adopted in reaction to new methods of disseminating disinformation: the internet in general and social media in particular.[30]

---

[22] Conseil constitutionnel, supra note 17.

[23] Conseil supérieur de l'audiovisuel, Propositions du Conseil supérieur de l'audiovisuel relatives à l'application du principe de pluralisme politique dans les média audiovisuels en période électorale 13 (Sept. 2015), https://perma.cc/FNZ3-E7RP.

[24] Belaich, supra note 21.

[25] C. électoral, art. L89.

[26] The original text uses the term *propagande*, which is, in French, a neutral term that could be best translated as "advocacy" or "advertising" in English.

[27] Conseil constitutionnel, *Quelles règles faut-il respecter sur les réseaux sociaux le jour et la veille du scrutin?* (undated), https://perma.cc/UDB8-9ZFC.

[28] Belaich, supra note 21.

[29] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (Dec. 22, 2018), https://perma.cc/QH5N-25MC. A companion law was adopted and signed at the same time: Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (Dec. 22, 2018), https://perma.cc/UK3K-YEQP. The latter only extends certain provisions of Loi n° 2018-1202 du 22 décembre 2018 to presidential elections.

[30] Bruno Studer, Assemblée nationale, Rapport fait au nom de la commission des affaires culturelles et de l'éducation sur la proposition de loi relative à la lutte contre la manipulation de l'information, No. 990, at 7–13 (May 30, 2018), https://perma.cc/X7ZB-HK32.

1. Transparency in Online Political Advertising in General

Under this new law, online platforms are required to establish a way for users to flag false information, especially when it is in content promoted for a third party.[31] This method of flagging fake news must be "easily accessible and visible."[32] Furthermore, online platforms are encouraged to take measures such as

- improving the transparency of their algorithms,
- promoting content from press agencies and radio and television services,
- fighting against accounts that massively disseminate fake information,
- informing users of the identity of the person(s) or organization(s) that bought paid content related to "a debate of national interest,"
- informing users of the nature, origin, and manner of broadcasting content, and
- educating people about the media and information.[33]

Online platforms must provide the Conseil supérieur de l'audiovisuel (CSA) (National Council on Audiovisual), France's main regulatory agency for radio and television broadcasting, with a yearly statement indicating what measures they took to fight against fake news.[34] The CSA is then supposed to publish regular reports on anti-fake-news measures taken by online platforms and their effectiveness.[35]

Additionally, online platform operators that use algorithms to organize the display of content related to "a debate of national interest" are required to publish statistics on how they work.[36] Online platform operators must specify, for every item of content: how often the item was accessed through direct access; how often it was accessed through the platform's recommendation, sorting, and referencing algorithms; and how often it was accessed through the platform's internal search function.[37] These statistics are to be published online and made accessible to anyone.[38]

Online platform operators must designate a legal representative in France to serve as a point of contact for the application of these provisions.[39]

---

[31] Loi n° 2018-1202 du 22 décembre 2018, art. 11.

[32] Id.

[33] Id.

[34] Id.

[35] Id. art. 12.

[36] Id. art. 14.

[37] Id.

[38] Id.

[39] Id. art. 13.

2. Transparency in Online Political Advertising During Election Campaigns

Some provisions of this new law aim to improve transparency for political advertising on the internet. Specifically, the law amended the Electoral Code to provide that online platforms with at least five million unique visitors per month must, during the three months preceding the first day of a month during which a national election is scheduled, and until the end of that election, provide users with "faithful, clear, and transparent information on the identity" of the person(s) or organization(s) that bought paid content related to "a debate of national interest."[40] Additionally, during that same time-frame, online platforms are required to give their users "faithful, clear and transparent information on the use of their personal data in the context of promoted information content related to a debate of national interest."[41] Furthermore, during the same time period, online platforms that are paid €100 (approximately US$110) or more per sponsored content must make the payment amount public.[42] Failure to abide by these requirements is punishable by up to one year in jail and a fine of €75,000 (approximately US$83,150).[43]

3. Other Measures to Stop Fake News During Election Periods

This new law also creates a new legal weapon to combat the dissemination of fake news during an election period. During the three months preceding the first day of an election month, and until the end of that election, a judge may order "any proportional and necessary measure" to stop the "deliberate, artificial or automatic and massive" dissemination of fake or misleading information online.[44] A public prosecutor, candidate, political party or coalition, or any person with standing may file the motion, and the court must rule within 48 hours.[45]

Additionally, the CSA may suspend the broadcasting license of an operator controlled by or under the influence of a foreign state if, during an election period, it broadcasts false information that could affect the election results.[46] While this measure is aimed at radio and television broadcasters, a suspension ordered by the CSA may apply to broadcasts on "any electronic communication service" (i.e., the Internet) as well as radio and television broadcasting.[47]

The CSA may also, after a first warning, withdraw the broadcasting license of a radio or television operator controlled by or under the influence of a foreign state, if it broadcasts content that harms

[40] C. électoral, arts. L163-1, D102-1; Décret No. 2019-297 du 10 avril 2019 relatif aux obligations d'information des opérateurs de plateforme en ligne assurant la promotion de contenus d'information se rattachant à un débat d'intérêt général, art. 1 (Apr. 10, 2019), https://perma.cc/7SEC-ZBZN.

[41] C. électoral, art. L163-1.

[42] Id. arts. L163-1, D102-1.

[43] Id. art. L112.

[44] Id. art. L163-2.

[45] Id.

[46] Loi n° 2018-1202 du 22 décembre 2018, art. 6; Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard), art. 33-1-1 (Sept. 30, 1986), https://perma.cc/67FR-KBF6.

[47] Loi n° 2018-1202 du 22 décembre 2018, art. 6; Loi Léotard, art. 33-1-1.

"the fundamental interests of the Nation."[48] This provision explicitly states that spreading false information to interfere with the proper functioning of institutions should be considered harmful to fundamental national interests.[49] The CSA may, in deciding to withdraw a broadcasting license, consider content that the broadcaster, or its subsidiary or parent organization, published on other communication services, such as the internet. However, the CSA may not base its decision to withdraw a license entirely on that factor.[50]

III. Other Government Actions

A. Counter-Measures during the 2017 Presidential Elections

There have been strong indications that Russia attempted to interfere with the French presidential election of 2017.[51] These alleged interference efforts include the last-minute release of a massive amount of leaked emails from the campaign of then-candidate Macron, among which were embedded fake emails.[52] However, it does not appear that foreign interference had any substantial impact on the election results. A key factor in countering foreign intervention efforts appears to have been the active role of two government agencies: the Commission Nationale de Contrôle de la Campagne Électorale en vue de l'Élection Présidentielle (CNCCEP) (National Commission for the Control of the Electoral Campaign for the Presidential Election), and the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) (National Cybersecurity Agency).[53] These agencies worked with the presidential candidates' campaigns to educate them on cybersecurity and warn them of specific threats and attacks.[54] Additionally, the CNCCEP issued a press release, shortly after the above-mentioned data leak, asking the media not to publish the content of the leaked emails and reminding them that disseminating false information can be a criminal offense.[55] Furthermore, law enforcement authorities reacted immediately to the leak, opening a criminal investigation within a few hours of its occurrence.[56]

B. Education

The law against the dissemination of false information adopted in December 2018 provides that French public schools should teach students how to navigate online information,

[48] Loi n° 2018-1202 du 22 décembre 2018, art. 8; Loi Léotard, art. 42-6.

[49] Id.

[50] Id.

[51] James Masters, *Fears of Russian Meddling as France Prepares to Go to the Polls*, CNN (Apr. 28, 2017), https://perma.cc/SPJ4-BM28.

[52] Alex Hern, Macron Hackers Linked to Russian-Affiliated Group Behind US Attack, The Guardian (May 8, 2017), https://perma.cc/6X2L-6MSP; Megha Mohan, Macron Leaks: The Anatomy of a Hack, BBC (May 9, 2017), https://perma.cc/U99V-NHCU.

[53] Jean-Baptiste Jeangène Vilmer, CSIS Briefs, *Successfully Countering Russian Electoral Interference* 2 (June 2018), https://perma.cc/8EMG-QP65.

[54] Id. at 3.

[55] Id. at 5.

[56] Id. at 4.

including the skills for "critical analysis of available information," and how to evaluate the reliability of information.[57]

C. Recommendations by the CSA

The CSA recently published a series of recommendations for online platform operators.[58] These recommendations largely reiterated those laid out in the Law No. 2018-1202 of Dec. 22, 2018, and include:

- The implementation of an accessible and visible reporting mechanism.[59]
- Ensuring the transparency of algorithms.[60]
- Promoting content from newspapers, news agencies, and from audiovisual communication services.[61]
- Detecting and countering accounts that disseminate false information on a massive scale.[62]
- Ensuring the transparency of promoted content.[63]
- Promoting media and information literacy.[64]

IV. Media Coordination

Some of the main online platform operators have taken steps to counter the spread of misinformation on social media. Much of their action is at the European level, most notably with the adoption of a Code of Practice on Disinformation, which is discussed in the section on the European Union. Some of the Europe-wide measures appear to have been at least partly inspired by French law. Facebook, for example, has stated that its measures to increase transparency in political advertising was "directly inspired by French regulation."[65] These measures include the requirement that political parties and election candidates register on the platform before being

[57] Loi n° 2018-1202 du 22 décembre 2018, arts. 16 to 19.

[58] CSA, Recommandation No. 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations (May 15, 2019), https://perma.cc/8PUT-GGCA, English version available at https://perma.cc/24C6-R6ET.

[59] Id. at 2.

[60] Id. at 3.

[61] Id. at 4.

[62] Id.

[63] Id.

[64] Id. at 5.

[65] Damien Leloup & Alexandre Piquard, Les pubs politiques sur Facebook en Europe seront accompagnées du message « payé par... », Le Monde (Jan. 28, 2019), https://perma.cc/BL7A-KKFF.

able to publish content seeking votes. Furthermore, Facebook has said that sponsored content will show who paid for it.[66]

Some operators appear to have taken country-specific approaches in addition to Europe-wide measures. Twitter, for example, announced that political campaigning ads would not be permitted in France.[67]

[66] Id.

[67] *Political Content in the European Union*, Twitter (undated), https://perma.cc/2WZS-GGTG.

Germany

Jenny Gesley
Foreign Law Specialist

SUMMARY In order to fight disinformation on social media platforms, in particular with regard to elections, Germany has several laws in place and is considering amending existing legislation to codify further duties to increase transparency. Depending on the facts of the case, there are a number of civil and criminal law provisions that may be applicable to safeguard individuals or the public from disinformation, especially on social networks. The best known is the Network Enforcement Act, which imposes high fines for noncompliance with existing legal duties to remove illegal content. In addition, a revision of the Interstate Treaty on Broadcasting is being considered, which would impose various duties on media intermediaries to increase transparency, among them a duty to identify social bots and a general duty for all electronic media to clearly identify a person who posts political, ideological, or religious advertisements.

The German federal government has also launched several campaigns and provided funding to foster media competence in German society in order to fight hate speech, cyber mobbing, and disinformation. In addition, Facebook Germany and the German Federal Office for Information Security have cooperated on several occasions before elections to verify social media accounts and institute other measures to increase cybersecurity.

I. Background

A. Disinformation on Social Media Platforms

In December 2016, the Parliamentary Research Services of the German Bundestag (parliament) published a report on dealing with the dissemination of disinformation ("fake news"), including the current legal situation and reform proposals.[1] The reason for the report was, among other things, a criminal complaint that the politician Renate Künast from the Green Party had filed against the authors of fake news published on Facebook.[2] According to news reports, several Facebook pages had posted a picture of the politician with a quote in which she allegedly commented on the recent highly publicized murder of a student and the arrest of a suspect in Freiburg, stating that "[e]ven though the traumatized young refugee has killed, he should be helped nonetheless."[3] The picture named the newspaper *Süddeutsche Zeitung* as a source for the quote. The politician filed a criminal complaint against the operators of a right-wing Facebook

[1] Wissenschaftliche Dienste, *Der Umgang mit Fake-News. Rechtslage und Reformansätze*, Report No. WD 10 - 3000 - 067/16 (Dec. 20, 2016), https://perma.cc/6W73-YKE7.

[2] Id. at 5; *Künast stellt Strafanzeige wegen Falschnachricht auf Facebook,* Frankfurter Allgemeine Zeitung (Dec. 10, 2016), http://perma.cc/M3KS-Z4B2.

[3] *Künast stellt Strafanzeige wegen Falschnachricht auf Facebook*, supra note 2.

page and against unknown persons.[4] She criticized the fact that it took Facebook three days to delete the false information.[5] Around the same time, reports about the dissemination of fake news during the 2016 United States (US) election campaign on Facebook and other social media platforms were published and fueled fears that the same could happen in the upcoming German federal elections in 2017.[6]

As a reaction to the spread of disinformation, in 2017, Germany passed the Network Enforcement Act, which explicitly aims to combat hate speech and fake news in social networks.[7] However, it should be noted that the Network Enforcement Act only entered into force on October 1, 2017, after the Federal Elections of September 24, 2017.[8] Likewise, the European Union (EU) in 2018 published an EU-wide voluntary Code of Practice on Disinformation and is planning to create an independent European network of fact-checkers to combat the spread of disinformation online.[9]

Furthermore, there have been calls from German parliamentarians to introduce a duty for media intermediaries, like social media platforms, to identify social bots that post information online, in order to increase transparency.[10] The state governments in Germany are currently working on a revision of the Interstate Treaty on Broadcasting which would include such a duty.[11] The draft also includes various other duties for media intermediaries to increase transparency.[12] The newest draft of the revision, for example, proposes a general duty for all electronic media to clearly identify a person who posts political, ideological, or religious advertisements.[13]

B. Free Speech Principles

Article 5 of the German Basic Law, the country's constitution, guarantees freedom of speech and freedom of the press, among other enumerated communication rights.[14] The communication rights are not restricted to Germans; they are applicable to "every person." In addition to all

[4] Id.

[5] Id.

[6] Wissenschaftliche Dienste, supra note 1, at 4.

[7] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerksdurchsetzungsgesetz] [NetzDG], Sept. 1, 2017, Bundesgesetzblatt [BGBl.] [Federal Law Gazette] I at 3352, https://perma.cc/4LPN-WS7Z (original), http://perma.cc/J86H-GTY4 (unofficial English translation).

[8] Id. art. 3.

[9] EU Code of Practice on Disinformation (Sept. 2018), http://perma.cc/456J-N5HV; *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Online Disinformation: A European Approach*, COM (2018) 236 final (Apr. 26, 2018), at 9, http://perma.cc/MMP9-4VP7.

[10] See, e.g., BR-Drs. 519/18, at 1, no. 2, https://perma.cc/K9EZ-56Q8.

[11] Rundfunkkommission der Länder, *Diskussionsentwurf für einen "Medienstaatsvertrag"* (July 2019), https://perma.cc/G5PK-8WQ7.

[12] Id. at 60, § 53 d.

[13] Id. at 66, § 58, para. 2.

[14] Grundgesetz [GG], May 23, 1949, BGBl. I at 1, as amended, art. 5, paras. 1 & 2, https://perma.cc/8UJX-HC4T (original), https://perma.cc/X9HV-VV32 (unofficial English translation).

natural persons, domestic legal persons may invoke it.[15] This also applies to foreign legal persons domiciled in the EU due to the bans on discrimination under EU law.[16]

Freedom of speech covers value judgments and statements of facts, if those statements of facts form the basis for an opinion. The term "opinion" is understood broadly. Expressions of a viewpoint, the taking of a position, or the holding of an opinion within the framework of intellectual dispute fall within its scope. If the statement "contributes to the intellectual battle of opinions on an issue of public concern," there is a presumption in favor of its admissibility. Untrue factual statements, however, fall outside the scope of freedom of expression.[17]

The communication freedoms are limited by general laws, provisions for the protection of young persons, and the right to personal honor.[18] The last two categories are generally seen as included in the category "general laws."[19] The Federal Constitutional Court defines "general laws" as laws that "do not prohibit or target the expression of an opinion as such," but rather "aim to protect a legal interest per se without regard to a specific opinion."[20] An example of a general law that might be relevant in the context of this report is, among others, the Criminal Code, in particular the provisions on insult or on the dissemination of ideas that violate human dignity.[21] However, these general laws have to be examined in light of the constitutional significance of the basic right they are restricting, meaning the limitations must themselves be interpreted restrictively in order to preserve the substance of the basic right, thus balancing these interests.[22]

II. Current and Pending Legislation

In Germany, there is no general law that prohibits the creation and dissemination of disinformation. However, depending on the facts of the case, there are a number of civil and criminal law provisions that may be applicable to safeguard individuals or the public from disinformation, in particular in social networks. The aforementioned Network Enforcement Act did not create new duties to delete content, but imposes fines if social media companies do not comply with existing duties. It relies on the violation of enumerated criminal law norms. In addition, new reporting requirements are established.

---

[15] Id. art. 19, para. 3; Bundesverfassungsgericht [BVerfG], Apr. 4, 1967, docket no. 1 BvR 414/64, para. 34, https://perma.cc/Y6GZ-2875.

[16] BVerfG, July 19, 2011, docket no. 1 BvR 1916/09, ECLI:DE:BVerfG:2011:rs20110719.1bvr191609, paras. 56 & 57, https://perma.cc/U4BD-MCW4 (original), https://perma.cc/ZNW4-3AYT (English translation).

[17] BVerfG, 61 BVerfGE 1, paras. 13-16, https://perma.cc/7B2V-44EQ (original), https://perma.cc/JU43-L7BC (unofficial English translation).

[18] GG, art. 5, para. 2.

[19] BVerfG, Nov. 4, 2009, docket no. 1 BvR 2150/08, ECLI:DE:BVerfG:2009:rs20091104.1bvr215008, para. 63, https://perma.cc/TXA9-4V97 (original), https://perma.cc/K5TL-D3DN (English translation (extract only)).

[20] BVerfG, 7 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 198 (Lüth decision), para. 36, https://perma.cc/2QZ5-5AWS (original), https://perma.cc/5M6Y-GRVX (unofficial English translation).

[21] StGB, §§ 185 et seq., § 130.

[22] BVerfG, supra note 20, para. 34.

A. Criminal Law

Under German criminal law, there are several provisions that prohibit the assertion or dissemination of personal information that is either false or cannot be proved to be true.[23] A requirement is that the information is capable of defaming a person or of negatively affecting public opinion of the person.[24] The crime of defamation is punishable with imprisonment not exceeding one year or a fine and, if it was committed publicly or through the dissemination of written materials, with imprisonment not exceeding two years or a fine.[25] If the defamation was done intentionally, the term of imprisonment may not exceed two years or a fine; if it was committed publicly, in a meeting, or through the dissemination of written materials, it will be punished with imprisonment not exceeding five years or with a fine.[26] If the defamation is directed towards a politician and it makes his or her public activities substantially more difficult, the punishment ranges from three months' to five years' imprisonment.[27] Social networks are generally considered public places, except when information is posted in closed groups.

Defamation and intentional defamation are only prosecuted upon the request of the victim.[28] The Public Prosecutor, however, will only open an investigation if it is in the public interest.[29]

In addition to a criminal prosecution, a person who has been defamed may also sue for libel in civil court and request a preliminary injunction.[30]

B. Media Law

The media law states that electronic information and communication services ("telemedia")[31] that provide journalistic content must conform to recognized journalistic standards, in particular when they completely or partially reproduce texts or visual contents of periodical print media.[32] This means that news must be "verified by the provider prior to their [sic] transmission with the

[23] StGB, §§ 186, 187.

[24] Id.

[25] Id. § 186.

[26] Id. § 187.

[27] Id. § 188.

[28] Id. § 194, para. 1.

[29] Strafprozeßordnung [StPO], Apr. 7, 1987, BGBl. I at 1074, 1319, as amended, §§ 374, 376, https://perma.cc/2J82-5LW3 (original), https://perma.cc/N6L5-3JE2 (unofficial English translation, updated through Apr. 23, 2014).

[30] Zivilprozessordnung [ZPO], Dec. 5, 2005, BGBl. I at 3202; BGBl. 2006 I at 431; BGBl 2007 I at 1781, as amended, §§ 935, 940, https://perma.cc/A5FE-YU8L (original), https://perma.cc/U3CT-U84L (unofficial English translation).

[31] Telemediengesetz [TMG], Feb. 26, 2007, BGBl. I at 179, as amended, § 1, para. 1, https://perma.cc/QG7Q-W28K (original), http://perma.cc/77GL-8FNJ (unofficial English translation, not updated).

[32] Staatsvertrag für Rundfunk und Telemedien [Rundfunkstaatsvertrag] [RStV], Aug. 31, 1991, as amended, art. 54, para. 2, https://perma.cc/7JJD-HE7S (original), https://perma.cc/562P-TNGH (unofficial English translation).

diligence appropriate to the circumstances concerning their content, source and truthfulness."[33] However, the law does not provide any consequences for a violation of journalistic standards. The only sanctions available to the German Press Council (Deutscher Presserat) are public reprimands.[34] In addition, the Press Code (Pressekodex) enforced by the German Press Council is only applicable to people who have voluntarily agreed to be bound by it, which is typically not the case for social media platforms or persons posting content on social media platforms.

C. Host Provider Liability

Host providers are generally not liable for false information published by third parties on their platforms as long as they do not have actual knowledge of the rights violation.[35] However, once they are notified of the rights violation, they must delete the content immediately in order to avoid liability.[36] The notification itself must be so specific and provide enough information that the host provider has a basis to qualify and verify the illegality of the posted information.[37] However, in practice, host providers have regularly ignored notifications, which was one of the reasons for enacting the Network Enforcement Act, described below.

D. Network Enforcement Act

One of the objectives of the Network Enforcement Act, adopted in 2017, was to fight "fake news" in light of the events during the 2016 US election campaign. The explanatory memorandum stated that

> fighting fake news on social networks [is] a priority. To do so requires improvements in law enforcement on social networks in order to promptly remove objectively criminal content, such as incitement to hatred, abuse, defamation or content that could lead to a breach of the peace by misleading authorities into thinking a crime has been committed.[38]

Surveys conducted on the deletion practices of social networks revealed that the voluntary commitments of social media platforms were insufficient. The government concluded that

> [s]ince the current mechanisms and the voluntary measures agreed on by social networks are inadequate and given the significant problems in enforcing the current law, it is necessary to introduce rules to make social networks comply on pain of a fine in order to

[33] Id.

[34] Presserat, Publizistische Grundsätze [Pressekodex] (2017), Complaints Procedure, § 12, para. 5, in conjunction with Press Code, § 16, http://perma.cc/2S8C-CB3L (original), http://perma.cc/AA56-Z4K7 (English translation).

[35] TMG, § 10.

[36] Id.

[37] Oberlandesgericht Hamburg [OLG Hamburg], Mar. 2, 2010, docket no. 7 U 70/09, 7 MultiMedia und Recht [MMR] 490, 491 (2010) (in German).

[38] BT-Drs. 18/12356, at 1, http://perma.cc/MD44-LD9G (original), https://perma.cc/SLD4-DACA (English translation).

> enable prompt, effective action against hate crime and other criminal content on the internet.[39]

During the whole legislative process, the Network Enforcement Act has been very controversial and has been criticized as unconstitutional, in particular with regard to free speech.[40] Several political parties have submitted proposals to amend or repeal the law.[41] However, none of the proposals have advanced very far yet.

As previously mentioned, the law in its current form does not create any new duties for social media platforms to remove content, but imposes high fines for noncompliance with existing legal obligations as outlined above (host provider liability).[42] It does, however, create new reporting requirements.

1. Scope of Application

The Network Enforcement Act is only applicable to social media networks that have two million or more registered users in Germany.[43] Social media networks are defined as "telemedia service providers that operate online platforms with the intent to make a profit and on which users can share content with other users or make that content publicly available."[44] The Act does not apply to platforms that post original journalistic content, or to email or messaging services.[45]

2. Removal of Illegal Hosted Content

The Act obligates the covered social media networks to remove content that is "clearly illegal" within twenty-four hours after receiving a user complaint.[46] If the illegality of the content is not obvious on its face, the social network has seven days to investigate and delete it. The seven-day deadline may be extended if additional facts are necessary to determine the truthfulness of the information or if the social network hires an outside agency to perform the vetting process (a recognized "Agency of Regulated Self-Regulation").

---

[39] Id. at 2.

[40] For a summary of the criticism, see Georg Nolte, *Hate-Speech, Fake-News, das »Netzwerkdurchsetzungsgesetz« und Vielfaltsicherung durch Suchmaschinen* 61 Zeitschrift für Urheber- und Medienrecht [ZUM] 552, 554 (2017) (in German).

[41] See, e.g., the draft act submitted by the Green Party, BT-Drs. 19/5950, http://perma.cc/FBW8-FJDP (amendment of the law), or the motion submitted by the Free Liberals (FDP), BT-Drs. 19/9225, https://perma.cc/3EZC-PEME, at 7, no. 13 (repeal of the law).

[42] See also Jenny Gesley, *Germany: Social Media Platforms to Be Held Accountable for Hosted Content Under "Facebook Act,"* Global Legal Monitor (July 11, 2017), http://perma.cc/KX9D-V6JL.

[43] NetzDG § 1, paras. 1, 2.

[44] Id. § 1, para. 1, sentence 1.

[45] Id. § 1, para. 1, sentences 2, 3.

[46] Id. § 3, para. 2, no. 2.

In order to determine whether an act is "illegal," the Network Enforcement Act refers to the Criminal Code, in particular to the provisions on dissemination of propaganda material or use of symbols of unconstitutional organizations, encouragement of the commission of a serious violent offense endangering the state, commission of treasonous forgery, public incitement to crime, incitement to hatred, and defamation, among others.[47]

3. Complaint Mechanism and Biannual Reports

The social media platforms are obligated to offer their users an easy and transparent complaint mechanism that is constantly available.[48] The decisions taken with regard to the complaint and the reasoning behind accepting or rejecting it must be communicated to the complainant and the affected user without undue delay.[49]

Social media networks that receive more than one hundred complaints about illegal content in a calendar year are required to publish a biannual report in German on how they deal with these complaints. The report has to be published in the German Federal Gazette and on the homepage of the social media network one month after the end of each half-year period.[50] The report must be easily identifiable, immediately accessible, and permanently available.[51] It must include information on the general efforts to prevent illegal actions on the platform, a description of the complaint procedure, the number of complaints received, the number and qualifications of employees who are handling the complaints, the network's association memberships, the number of times an external party has been used to decide the illegality of the content, the number of complaints that led to the content being deleted, the time it took to delete the content, and measures that were taken to inform the complainant and the member who posted the deleted content.[52]

4. Fines

A social media network that intentionally or negligently violates certain of the above-mentioned obligations may be fined up to €50million (about US$57.8 million) by the German Federal Office of Justice.[53] If the Federal Office of Justice wants to fine a company because it considers the content

[47] Id. § 1, para. 3.

[48] Id. § 3, para. 1.

[49] Id. § 3, para. 2, no. 5.

[50] Id. § 2, para. 1.

[51] Id.

[52] Id. § 2, para. 2.

[53] Id. § 4, in conjunction with Gesetz über Ordnungswidrigkeiten [OwiG], Feb. 19, 1987, BGBl. I at 602, as amended, http://perma.cc/NLL2-TRBA (original), http://perma.cc/2BL2-W7VF (unofficial English translation). The Federal Office of Justice is an agency that forms part of the Federal Ministry of Justice and Consumer Protection.

that was not deleted to be illegal, it must first obtain a court decision to this effect.[54] The court decision is final and binding on the Federal Office of Justice.[55]

5. Recent Developments

In July 2019, the Federal Office of Justice imposed a fine of €2 million (about US$2.2 million) on Facebook Ireland Ltd. for violating its reporting obligations under the Network Enforcement Act.[56] The Federal Office of Justice alleges that Facebook's July 2018 report lists only a fraction of the complaints filed by users about unlawful content, thereby "affect[ing] the degree to which meaningful, disaggregated information has been provided on the measures taken." In addition, Facebook is accused of reporting inaccurately on measures to inform complainants and users. Facebook has announced it will file an appeal.[57]

E. Revision of the Interstate Broadcasting Treaty

The German states are currently discussing a revision of the Interstate Broadcasting Treaty and are soliciting public comments.[58] The draft proposes to expand the scope of the Interstate Broadcasting Treaty to cover not only traditional broadcasters, but also media intermediaries like social media platforms. The name change to "Interstate Media Treaty" would reflect that change. An earlier draft from 2018 defined "media intermediary" and contained a nonexhaustive list of media intermediaries. A media intermediary is defined as "every telemedium that aggregates, selects, and presents for general use journalistic-editorial third party offers, without summarizing it to one overall offer. Media intermediaries are in particular search engines, social networks, app portals, user generated content portals, blogging portals, and news aggregators."[59] In order to remain open to technological changes, however, the newest draft from July 2019 does not contain that list anymore.[60]

The draft includes various general duties for media intermediaries to increase transparency.[61] In particular, the Treaty would impose a duty on media intermediaries to identify social bots that post information on social media networks if the user account appears to have been opened for a natural person. The post or message needs to disclose in an easily readable way that it was

[54] NetzDG, § 4, paras. 4, 5.

[55] Id. § 4, para. 5.

[56] Press Release, Federal Office of Justice, Federal Office of Justice Issues Fine Against Facebook (July 3, 2019), https://perma.cc/SVC5-KFTN.

[57] Jenny Gesley, *Germany: Facebook Found in Violation of "Anti-Fake News" Law*, Global Legal Monitor (Aug. 20, 2019), https://perma.cc/T5PM-H3G7.

[58] Rundfunkkommission der Länder, supra note 11; Press Release, Landesregierung Rheinland-Pfalz, Zweite Anhörung zum Medienstaatsvertrag am 03. Juli 2019 gestartet (July 3, 2019), https://perma.cc/A7CK-T6WJ.

[59] Rundfunkkommission der Länder, supra note 11, at 11, § 2, no. 13 b (middle column).

[60] Id., right column.

[61] Id. at 60, § 53 d.

automatically generated and posted by a computer program.[62] Failure to fulfill these duties may result in administrative fines.[63]

In general, all broadcasters are forbidden from broadcasting advertisements of a political, ideological, or religious nature.[64] There are specific rules that allow campaign advertisements before an election.[65] This general prohibition, however, does not apply to telemedia.[66] The newest draft of the revision therefore proposes a general duty for all telemedia to clearly identify the person who posts political, ideological, or religious advertisements.[67]

III. Other Government Actions

The German federal government has launched several campaigns and provided funding to foster media competence in German society to fight hate speech, cyber mobbing, and disinformation, in particular for children and young people. Examples are the initiative "Ein Netz für Kinder," a guideline for parents and caretakers on how to introduce children to the internet,[68] "Schau Hin!," an online guide for parents on traditional media, the internet, social media, smartphones, and similar topics,[69] and "Demokratielabore,"[70] workshops designed to inform young people about hate speech, participation, and involvement in society, among others.[71] The Federal Agency for Civic Education also offers various resources for adults in order to foster media competency, with a focus on disinformation and belligerent and inciting content.[72]

In addition, the German federal government coordinates with state governments and at the European level to create effective measures against hate speech and disinformation.[73] It also supports the development of regional German centers and professional communication instruments as a countermeasure to hybrid disinformation offline and online in Germany and abroad.[74]

---

[62] Id. § 53 d, para. 4, § 55 para. 3.

[63] Id. at 39, § 49, para. 1, nos. 12b-12f (right column).

[64] Staatsvertrag für Rundfunk, supra note 32, § 7, para. 9.

[65] Id. § 42.

[66] Id. § 1, para. 1.

[67] Rundfunkkommission der Länder, supra note 11, at 66, § 58, para. 2 (right column).

[68] Bundesministerium für Familie, Senioren, Frauen und Jugend, *Ein Netz für Kinder* (14th ed. June 2016) (in German) https://perma.cc/C8PG-UX7B.

[69] "Schau Hin! ," https://perma.cc/B6EG-99QM.

[70] *Demokratielabore* (2017-2018), https://perma.cc/CVF4-WMTC.

[71] BT-Drs. 19/6970, at 11, https://perma.cc/LCZ9-BYSG.

[72] Id. at 12.

[73] Id. at 13.

[74] Id. at 12.

IV. Media Coordination

Facebook Germany has cooperated with the German Federal Office for Information Security on several occasions before the 2017 federal elections and since 2018 for future elections to verify social media accounts and institute other measures to increase cybersecurity.[75]

[75] BT-Drs. 19/8056, at 2-3, nos. 2-4, https://perma.cc/G3EH-Z24E.

India

Tariq Ahmad
Foreign Law Specialist

SUMMARY The problem of "fake news" and misinformation appears to be a substantial problem in India. However, unlike the United States, where the focus is mostly on foreign based misinformation campaigns, India has more of a domestic misinformation problem involving major political parties and associated "cyber-army" groups. There is no specific provision in Indian law that specifically deals with fake news. However, there are several offenses in India's Penal Code that criminalize certain forms of speech that may be relevant to fake news and may apply to online or social media content, including the crimes of sedition and promoting enmity between different groups.

The Information Technology Act 2000, which regulates electronic commerce and provides for certain cybercrimes, contains a provision (section 66A) prohibiting the dissemination of information that a person knows to be false by means of a computer resource or a communication device for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, but this provision has been struck down as unconstitutional by the Supreme Court of India. The 2000 Act and the Information Technology (Intermediaries Guidelines) 2011 also establish limited immunity for social media and other internet companies for any illegal content posted by third parties and outline the due diligence to be observed by intermediary companies for removing such content. In 2018, new draft rules were proposed by the government that seek to curtail the misuse of social networks and increase accountability.

Social media companies voluntarily agreed to implement the silent period on social media platforms and to process reported violations within three hours, among other measures, during the 2019 general elections. The Election Commission of India has issued instructions on social media use during election campaigns that require candidates to provide certain information about their social media accounts; obtain precertification or approval of their political advertisements; and report expenditure on campaigning through the internet, including via social media websites.

I. Background

The problem of "fake news" appears to be significant in India with some commentators even describing it as a "public health crisis."[1] 'Indians were most likely to encounter fake news and internet hoaxes among the twenty-two countries surveyed as part of Microsoft's Third Digital Civility Index.[2] An article in the *Atlantic* describes the situation as follows:

[1] Samir Patil, Op-Ed., *India Has a Public Health Crisis. It's Called Fake News,* N.Y. Times (Apr. 29, 2019), https://perma.cc/S5HU-UK4Q.

[2] *Microsoft Releases Digital Civility Index on Safer Internet Day*, Microsoft News Center India (Feb. 5, 2019), https://perma.cc/545B-7YVN.

> India is facing information wars of an unprecedented nature and scale. Indians are bombarded with fake news and divisive propaganda on a near-constant basis from a wide range of sources, from television news to global platforms like Facebook and WhatsApp. But unlike in the United States, where the focus has been on foreign-backed misinformation campaigns shaping elections and public discourse, the fake news circulating here isn't manufactured abroad. Many of India's misinformation campaigns are developed and run by political parties with nationwide cyberarmies; they target not only political opponents, but also religious minorities and dissenting individuals, with propaganda rooted in domestic divisions and prejudices. The consequences of such targeted misinformation are extreme, from death threats to actual murders—in the past year, more than two dozen people have been lynched by mobs spurred by nothing more than rumors sent over WhatsApp.[3]

Fake news spread over Whatsapp, India's most popular messaging platform, has been of particular concern. According to one BBC report Whatsapp had become "a vehicle for misinformation and propaganda" where both the governing Bharatiya Janata Party (BJP) and the major opposition Congress Party were accused of "spreading false or misleading information" ahead of the 2019 general election.[4] Following a suicide bombing against Indian security forces in Kashmir in 2019, "a message began circulating in WhatsApp groups across the country. It claimed that a leader of the Congress Party, the national opposition, had promised a large sum of money to the attacker's family, and to free other 'terrorists' and 'stone pelters' from prison, if the state voted for Congress in upcoming parliamentary elections." The message was "aimed at painting the BJP's main national challenger [the Congress Party] as being soft on militancy" in the disputed territory of Kashmir.[5] Another incident of fake news highlighted by news reports involved an attempt to show that the BJP party was "indulging in war mongering for electoral gains":[6]

> Two weeks after a suicide bombing in Kashmir in February killed 40 Indian paramilitary policemen, a Facebook user called Avi Dandiya posted a live video in which he played a recording of a call purportedly involving India's home minister, the president of the ruling Bharatiya Janata Party (BJP) and an unidentified woman. The trio could be heard talking about arousing nationalist sentiment ahead of India's general election, with the BJP president allegedly saying in Hindi: "We agree that for election, we need a war". Within 24 hours, one of Facebook Inc's fact-checking partners in India, BOOM, exposed Dandiya's video as fake. An analysis on BOOM's website said the video was created by splicing audio from older political interviews.[7]

---

[3] Snigdha Poonam & Samarth Bansal, *Misinformation Is Endangering India's Election*, The Atlantic (Apr. 1, 2019), https://perma.cc/Y39M-KGWU.

[4] Kevin Ponniah, *WhatsApp: The 'Black Hole' of Fake News in India's Election*, BBC News (Apr. 6, 2019), https://perma.cc/5YJS-ZH2A

[5] Poonam & Bansal, supra note 3.

[6] Anjana Pasricha, *Fake News Inundates India Social Media Ahead of Election*, Voice of America (Apr. 3, 2019), https://perma.cc/798C-YMWE

[7] Sankalp Phartiyal & Aditya Kalra, *Despite Being Exposed, Fake News Thrives on Social Media ahead of India Polls,* Reuters (Apr. 3, 2019), https://perma.cc/URB7-H96V.

Freedom of expression is mentioned in the preamble of India's Constitution and the right is protected under article 19, which states that "[a]ll citizens shall have the right . . . to freedom of speech and expression."[8] This right is not absolute and is subject to "reasonable restrictions" "in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence."[9]

In the 2015 case of *Shreya Singhal v. Union of India*,[10] which tested the scope of the "reasonable restrictions" standard, the Supreme Court of India struck down section 66A of the Information Technology Act, 2000,[11] holding that "the [section's] prohibition against the dissemination of information by means of a computer resource or a communication device intended to cause annoyance, inconvenience or insult did not fall within any reasonable exceptions to the exercise of the right to freedom of expression."[12] "It is clear," the Court said, "that Section 66A arbitrarily, excessively and disproportionately invades the right of free speech and upsets the balance between such right and the reasonable restrictions that may be imposed on such right."[13] The Court also stated that the definition of offenses under the section were both "open-ended and undefined"[14] and that "[t]he information disseminated over the Internet need not be information which 'incites' anybody at all. Written words may be sent that may be purely in the realm of 'discussion' or 'advocacy' of a 'particular point of view.' "[15] However, in other cases, the Supreme Court of India has upheld restrictions on free speech such as in the case of *Subramanian Swamy v.*

[8] India Const. art. 19(1)(a), https://perma.cc/MCD8-7XAT.

[9] Id. art. 19(2).

[10] Shreya Singhal v. Union of India, Writ Petition (Crim.) No. 167 of 2012 (Mar. 24, 2015), https://perma.cc/X8QZ-7TV8.

[11] Information Technology Act, 2000, No. 21, https://perma.cc/4TWL-Q4MY. Section 66A provided as follows:

> 66A. Punishment for sending offensive messages through communication service, etc.–Any person who sends, by means of a computer resource or a communication device,–
>
> (a) any information that is grossly offensive or has menacing character; or
>
> (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;
>
> (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
>
> shall be punishable with imprisonment for a term which may extend to three years and with fine.

[12] *Singhal v. Union of India: Case Analysis*, Columbia Global Freedom of Expression, https://perma.cc/FF8S-AH2G.

[13] Shreya Singhal v. Union of India, Writ Petition (Crim.) No. 167 of 2012, at 72.

[14] Id. at 62.

[15] Id. at 38-39.

Union of India,[16] which upheld the constitutionality of the criminal defamation sections of the Indian Penal Code

II. Current and Pending Legislation

A. Penal Code

No provision in Indian law specifically deals with "fake news." However, the following offenses under India's Penal Code[17] criminalize certain forms of speech that may constitute "fake news" and apply to online or social media content:

- Section 124A. Sedition: "Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with [various combinations of terms of imprisonment and/or fines]."

- Sections 153A. Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.

- Section 292. Sale, etc. of obscene books.

- 295A. Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs. "Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India, by words, either spoken or written, or by signs or by visible representations or otherwise, insults or attempts to insult the religion or the religious beliefs of that class, shall be punished [with a fine and/or imprisonment]."

- Section 499. Defamation. "Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person."

- Section 503. Criminal intimidation.
- Section 504. Intentional insult with intent to provoke breach of the peace.
- Section 505. Statements conducing to public mischief.

The Law Commission of India in its 267th Report recommended adding two new provisions to the Penal Code to further discourage hate speech. The report suggests that a section 153C be

[16] Association for Progressive Communications (APC), *State of the Internet in Asia: The Case of India, Malaysia and Pakistan* 21 (2017), https://perma.cc/KV6N-ZRR4.

[17] Indian Penal Code, No. 45 of 1860, https://perma.cc/49VP-ZC6C.

added to prohibit incitement to hatred and a section 505A to prohibit speech that causes fear, alarm, or provocation of violence.[18]

B. The Information Technology Act, 2000

1. Cyber Crimes

The Information Technology (IT) Act[19] regulates electronic commerce and provides for certain cybercrimes. Offenses, listed in Chapter XI of the Act, specify punishments for publishing obscene[20] and sexually explicit material.[21] As noted above, the IT Act had a section 66A[22] that could have been applicable to instances of fake news, but has since been struck down by the Supreme Court on the ground that did not fall within any of the reasonable exceptions to the exercise of the constitutional right to freedom of expression. As described by the Court, the provision had prohibited "the dissemination of information by means of a computer resource or a communication device intended to cause annoyance, inconvenience or insult."[23]

2. Immunity of Intermediaries and Removing Content

The Information Technology (Intermediaries Guidelines) Rules, 2011 are a set of subsidiary rules under the Act.[24] Rule 3 establishes the due diligence to be observed by intermediary companies, defining "intermediary," "with respect to any particular electronic records, [as] any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."[25] Rule 3(1) requires intermediaries to publish the rules and regulations, privacy policies, terms and conditions, and user agreement for using the computer resource, while Rule 3(2) requires that these documents

> (2) . . . inform the users . . . not to host, display, upload, modify, publish, transmit, update or share any information that—
>
> (a) belongs to another person and to which the user does not have any right to;
>
> (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically

[18] Law Commission of India, Report No. 267, *Hate Speech* 50 (Mar. 2017), https://perma.cc/692Y-AHC9.

[19] Information Technology Act, No. 21 of 2000, https://perma.cc/466L-Z757.

[20] Id. § 67.

[21] Id. §§ 67A-67B.

[22] Id. § 66A.

[23] Shreya Singhal v. Union of India, Writ Petition (Crim.) No. 167 of 2012 (Mar. 24, 2015), https://perma.cc/X8QZ-7TV8.

[24] Information Technology (Intermediaries Guidelines) Rules, 2011, https://perma.cc/L4N4-QV66. For a comprehensive overview of the rules see Suneeth Katarki et al., IndusLaw, *India: The Draft Information Technology Intermediaries Guidelines (Amendment) Rules, 2018*, Mondaq.com (Feb. 19, 2019), https://perma.cc/A8GJ-V3QX.

[25] InformationTechnology (Intermediaries Guidelines) Rules, 2011, supra note 24, § 2(w).

> objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
> (c) harm minors in any way;
> (d) (d) infringes any patent, trademark, copyright or other proprietary rights;
> (e) violates any law for the time being in force;
> (f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
> (g) impersonate another person;
> (h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;
> (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

Section 79 of the IT Act grants limited immunity to intermediaries for any illegal content posted by third parties:

> 79. Exemption from liability of intermediary in certain cases.–(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

However, under this section and Rule 3(4) of the Information Technology (Intermediaries Guidelines) 2011, if an intermediary obtains knowledge by itself, through a writing or an electronically signed email from the affected person, or upon notification by the government of any illegal content posted on its site, it is obligated to remove such content and failing to do so will cause it to lose its immunity from being sued:

> (3) The [immunity] provisions of sub-section (1) shall not apply if—
>
> *(a)* the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
>
> *(b)* upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.[26]

The Intermediary Rules stipulate that an intermediary has thirty-six hours to remove the content.[27] The Supreme Court of India has held, however, that intermediaries could be held liable for "failing to comply with legal requests sent by government agencies or . . . a court order."[28] The

[26] Information Technology Act, No. 21 of 2000, § 79(3).

[27] InformationTechnology (Intermediaries Guidelines) Rules, 2011, supra note 24, § 3(4).

[28] APC, supra note 16, at 20 (citing Shreya Singhal v. Union of India, (2015) A.I.R. 1523 (S.C.)).

intermediary will not be held liable if he or she "chooses not to act in response to a private takedown notice – i.e., a complaint sent by an individual or other non-governmental entity."[29]

In 2018, a calling attention motion[30] on the misuse of social media platforms and the spreading of fake news was admitted in the Rajya Sabha, the upper house of India's National Parliament. The Minister of Electronics and Information Technology responded to the motion on July 26, 2018, and "made a detailed statement where he inter alia conveyed to the House the resolve of the Government to strengthen the legal framework and make the social media platforms accountable under the law."[31] Subsequently, the Ministry prepared the draft Information Technology (Intermediary Guidelines (Amendment) Rules 2018[32] which would amend the rules notified in 2011. Under the draft rules intermediaries would be required to proactively monitor and filter unlawful content[33] and provide for the traceability of users.[34]

Additions are made to Rule 3(2) so intermediaries are required to inform their users against hosting any material that may also threaten critical information infrastructure, public health or safety.[35] In the draft, the old Rule 3(4) (receiving actual knowledge from affected person/containing the thirty-six-hour rule) would be removed and a new Rule 3(4) would be added mandating that intermediaries send a monthly notification to their users reminding them of the consequences of noncompliance with the provisions of the rules and regulations, user agreement, and privacy policy.[36] Rule 3(8) and Rule 3(9) of the Draft Rules would require an intermediary, upon receiving actual knowledge in the form of a court order or on being notified by the government, to remove or disable access to material that may be lawfully restricted under article 19(2) of the Indian Constitution within twenty-four hours. Material subject to such restriction includes that which adversely impacts the interests of the sovereignty and integrity of India, the security of the nation, friendly relations with other countries, public order, or decency and morality, or that which constitutes contempt of court, defamation or incitement to an offense, on a computer resource[37] The intermediary must "deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information or content."[38]

---

[29] Id. at 64-65.

[30] Calling attention motions are used to highlight matters of urgent public importance. *Calling Attention*, Rajya Sabha (Feb. 2005), https://perma.cc/2Q26-FLPS.

[31] *Comments / Suggestions Invited on Draft of "The Information Technology [Intermediary Guidelines (Amendment) Rules] 2018,* Ministry of Electronics & Information Technology, https://perma.cc/3SP2-8MFN.

[32] Information Technology [Intermediaries Guidelines (Amendment) Rules 2018, https://perma.cc/E9M9-BNWU.

[33] Id. Rule 3(9).

[34] Id. Rule 3(8).

[35] Id. Rule 3(2).

[36] Id. Rule 3(4).

[37] Id. Rule 3(8).

[38] Id. Rule 3(9).

Rule 3(5) of the draft rules would allow government agencies to ask for assistance concerning security of the state or cyber security and further require intermediaries to enable tracing of the originators of information on its platforms upon a lawful request by a government agency.[39] Critics have said this could undermine the end-to-end encryption and privacy provided to users by platforms like Whatsapp.[40]

3. Blocking Content

Section 69A of the Information Technology Act allows the Central Government to issue directions to block content on certain grounds, including to prevent incitement for the commission of a cognizable offense. Procedures and safeguards to which the government must adhere when doing so are set forth in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (known as the Blocking Rules).[41]

C. Internet Shutdowns

According to the Freedom House, a US-based research and advocacy organization, India is the world leader in internet shutdowns, with one hundred reported shutdowns in 2018 alone.[42] The Soft Freedom Law Center India has reported that, in June 2019, eleven instances of internet shutdowns were reported in India. Of those eleven cases, seven were ordered in the areas of Jammu and Kashmir, while West Bengal only experienced two internet shutdowns.[43] In Jammu and Kashmir the number of internet shutdowns more than doubled each year from 2015 to 2018. This is expected to increase again in 2019.[44] Governments in India have used internet shutdowns to deal with fake news on a number of occasions. In June 2018 in northeastern India internet access was cut "after mobs beat three people to death in lynchings sparked by rumours spread on smartphones."[45] On August 2018, a riot broke out over rumors that a fourteen-year-old girl had been attacked:

> On August 25, hundreds of people took to the streets of the small Indian district of Banda, part of the Northern region of Shahjahanpur, in protest at reports a guard had hit her when she tried to set up her market stall outside the local Gurdwara. The action prompted anger from the local Sikh and Hindu communities who faced off. Stones were thrown by the two

[39] Id. Rule 3(5).

[40] Purushotham Kittane, *Under India's New Intermediary Rules, Fundamental Rights Take Backstage*, Oxford Human Rights Hub (Mar. 15, 2019), https://perma.cc/PJN9-TBTK.

[41] Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, https://perma.cc/6THW-MKHW.

[42] Megha Bahree, *India Leads the World in the Number of Internet Shutdowns: Report,* Forbes (Nov. 2, 2018), https://perma.cc/D2AQ-NC2C.

[43] Soumyarendra Barik, *India Saw 11 Internet Shutdowns in June, 59 so far in 2019,* Medianama (July 2, 2019), https://perma.cc/X397-55QW.

[44] C.K. Hickey, *India Is the World's Leader in Internet Shutdowns*, Foreign Policy (Aug. 5, 2019), https://perma.cc/6EJX-LREV.

[45] *Indian State Cuts Internet after Lynchings over Online Rumours*, The Guardian (June 29, 2018), https://perma.cc/S53S-TMYA.

> groups, damaging cars and injuring 12 people. Police officers in helmets and body armour fired tear gas into the crowd to try and regain control. The incident was captured by media reports and eyewitness recordings. Days later, police brought charges of rioting, damage to public property and arson against 70 people. A peacekeeping meeting between the two religious communities was also held. Then, on August 27, local authorities ordered a shutdown of mobile internet connections in the area from 06:00 until 14:00 to stop the spread of online rumours about the alleged attack and subsequent unrest. But the real target of the shutdown wasn't the internet as a whole, it was WhatsApp.[46]

Several laws are used to support internet shutdowns, as described below.

1. Section 144 of the Code of Criminal Procedure, 1973

In India, internet shutdowns are normally pursued on the basis of section 144 of the Code of Criminal Procedure, 1973,[47] which is "usually invoked to prevent riots and enforce curfew, and maintain law and order in a communally charged atmosphere, where there could be a danger to the physical safety of a group of people based on their religious, caste, linguistic or ethnic identity."[48] The section provides that magistrates specifically empowered by the state government may, by written order, direct any person to abstain from a certain acts or take certain orders regarding property in their possession or management. Proceeding under section 144(1) is permissible when an "immediate prevention or speedy remedy is desired", and the magistrate believes such action is likely to prevent obstruction, annoyance, or injury to any person lawfully employed; or danger to human life, health, or safety; a disturbance of the public tranquility; or a riot or "affray" (melee).[49] Such orders may be issued ex parte[50] and may be directed to a particular individual, person residing in a particular place or area, or the general public frequenting or visiting a particular place or area.[51] They initially remain in force for no more than two months but may be extended for an additional six months period if the state government believes an extension is necessary to prevent danger to human life, health, or safety, or to prevent a riot or an affray.[52]

A Software Freedom Law Center report notes that operative words used in the provision, such as "obstruction," "annoyance," "disturbance to public tranquillity," or "affray," are not defined

[46] Matt Burgess, *To Fight Fake News on WhatsApp, India Is Turning Off the Internet*, Wired (Oct. 18, 2018), https://perma.cc/Q9J6-KW3P.

[47] Code of Criminal Procedure, 1973, Act No. 2 of 1974, https://perma.cc/7DLF-6SL7, discussed in APC, supra note 16, at 87.

[48] Siddharth Narrain, *Internet Shutdowns: Background and Use of Section 144, Code of Criminal Procedure, 1973*, Socio-legal Rev. (Mar. 11, 2018), https://perma.cc/MW79-YDDY.

[49] Code of Criminal Procedure, 1973, § 144(1).

[50] Id. § 144(2).

[51] Id. § 144(3).

[52] Id. § 144(4).

under the Code of Criminal Procedure or any other legislation, thus opening the statutory provision to inconsistent interpretations.[53]

Use of section 144 for internet shutdowns "was heavily favored at least until the Telecom Suspension Rules were notified in 2017, though it has continued to be intermittently used even afterwards."[54] According to the Software Freedom Law Center, the provision "has traditionally been used to issue curfews and dismiss unlawful assemblies during widespread civil unrest."[55]

2. Section 5(2) of the Indian Telegraph Act, 1885

Section 5 of the Indian Telegraph Act, 1885,[56] addresses the power of the government to "take possession of licensed telegraphs and to order interception of messages." According to the Software Freedom Law Center the section "has also been invoked multiple times to order temporary Internet service disruptions,"[57] and it is used to "prevent the transmission of any telegraphic message or class of messages during a public emergency or in the interest of public safety"[58] if it is necessary or expedient for the sake of the sovereignty or integrity of India, the security of the state, the preservation of friendly relations with foreign states, public order, or preventing incitement to the commission of an offense.[59] Because the term "telegraph" is broadly defined in the Act, subsection 5(2) can also be used to justify internet shutdowns.[60] The reasoning for invoking shutdown powers under subsection 5(2) must be recorded in writing.

3. Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017

The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017,[61] were promulgated under the India Telegraph Act, 1885, to regulate the temporary suspension of telecom services in cases of a public emergency or for public safety,[62]

In accordance with Rule 2, directions to suspend telecom services can only be issued by an order made by the Secretary of the Government of India in the Ministry of Home Affairs in the case of

[53] Software Freedom Law Center, *Living in Digital Darkness: A Handbook on Internet Shutdowns in India* 57 (May 2018), https://perma.cc/KD8V-3APH.

[54] Id. at 8.

[55] Id. at 9.

[56] Indian Telegraph Act, 1973, No. 13 of 1885, https://perma.cc/RE5G-GR8S.

[57] Software Freedom Law Center, supra 53, at 12.

[58] Id. at 13.

[59] Indian Telegraph Act, 1973, § 5(2).

[60] Software Freedom Law Center, supra 53, at 13.

[61] Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, Gazette of India, pt. II, § 3(i) (Aug. 8, 2017), https://perma.cc/PG47-UDL5.

[62] Software Freedom Law Center, supra 53, at 13.

an action by the government of India[63] or by the Secretary to the State Government in-charge of the Home Department in the case of actions by a state government. In unavoidable circumstances where obtaining prior direction is not feasible, the order may be issued by an officer above the rank of a Joint Secretary to the Government of India.[64] An order to suspend telecom services is subject to confirmation by the competent authority within twenty-four hours of issuance and ceases to exist if confirmation from the competent authority is not received within this period.[65] Rule 2(5) calls for the creation of a Review Committee constituting of officials from the Central Government and state governments. The Review Committee is to meet within five working days of the issuance of directions for suspension services caused by public emergencies or public safety concerns. All findings discussed in Review Committee hearings must be recorded.[66] The Review Committee will issue findings as to whether the orders issued are in accordance with the provisions of section 5(2) of the Indian Telegraph Act.

D. Election Commission of India & the Representation of the People Act, 1951

1. Forty-Eight-Hour Silence Period

The Representation of the People Act, 1951, India's main election law, regulates the conduct of elections to the Houses of Parliament and to the legislatures of each Indian state. The Act prohibits advertising and campaigning on TV and other electronic media by candidates and political parties during the "silent period," which is forty-eight hours before the end of polling.[67] According to the Election Commission of India (ECI) individuals are not prohibited from expressing their private opinions during the blackout period, however.[68]

A Committee established by the ECI to review and suggest changes to the silent-period provision and other relevant guidance submitted its report in January 2019,[69] proposing an expansion of the scope of the forty-eight-hour ban to cover print media and "intermediaries" as defined in section 2(w) of the Information Technology Act. In a letter to the Law Ministry, the Committee explained that the change was sought in order to "bring print media, news portals and social media under the purview of the 48-hour ban on electioneering prior to the conclusion of poll [sic]," according to news reports.[70]

---

[63] Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, supra note 61, Rule 2(1).

[64] Id.

[65] Id.

[66] Id. Rule 2(5).

[67] Representation of the People Act, No. 43 of 1951, § 126, https://perma.cc/L7FX-SFMK.

[68] Kanchan Chaudhari, *We Can't Stop Individuals from Using Social Media 48 Hours before Polls, ECI Tells Bombay HC*, Hindustan Times (Jan. 12, 2019), https://perma.cc/GX7H-EL62.

[69] Press Release, Election Commission, Report of the Committee on Section 126 of the Representation of the People Act, 1951 Submitted to the Commission (Jan. 10, 2019), https://perma.cc/9Q5E-ZMBG.

[70] *Silence Period Explained: 48 Hours before Polls, Use of Digital or Television Media Verboten for Political Campaigning*, Firstpost (Apr. 17, 2019), https://perma.cc/TRM5-WBHE.

2. Model Code of Conduct (MCC)

The Model Code of Conduct (MCC)[71] is a set of guidelines issued by the ECI to "regulate political parties and candidates prior to elections, to ensure free and fair elections."[72] The MCC becomes operational from the date that the "election schedule is announced till the date that results are announced."[73] In terms of its enforceability PRS Legislative Research states that

> [t]he MCC is not enforceable by law. However, certain provisions of the MCC may be enforced through invoking corresponding provisions in other statutes such as the Indian Penal Code, 1860, Code of Criminal Procedure, 1973, and Representation of the People Act, 1951. The Election Commission has argued against making the MCC legally binding; stating that elections must be completed within a relatively short time (close to 45 days), and judicial proceedings typically take longer, therefore it is not feasible to make it enforceable by law. On the other hand, in 2013, the Standing Committee on Personnel, Public Grievances, Law and Justice, recommended making the MCC legally binding. In a report on electoral reforms, the Standing Committee observed that most provisions of the MCC are already enforceable through corresponding provisions in other statutes, mentioned above. It recommended that the MCC be made a part of the Representation of the People Act, 1951.[74]

In March 2019, in anticipation of the general election, the ECI published the *Manual on the Model Code of Conduct*[75] as guidance for political parties and candidates, including information on the Model Code, enabling law, instructions, and court decisions.[76] The Manual makes mention of a Compendium of Instructions on Election Expenditure Monitoring (February, 2019)[77] and Instructions of the Commission with respect to use of Social Media in Election Campaigning.[78] These instruction on social media were issued on October 25, 2013, and contain guidelines on "information to be given by candidates about their social media accounts," precertification of political advertisements, and "expenditure on campaigning through [the] internet including social media websites."[79] More information on them are detailed below.

---

[71] Election Commission of India, Model Code for the Guidance of Political Parties and Candidates, https://perma.cc/34BQ-WMTW.

[72] Roshni Sinha, *Model Code of Conduct and the 2019 General Elections*, PRS Legislative Research (Mar. 11, 2019), https://perma.cc/63XM-TWSS.

[73] Id.

[74] Id.

[75] Election Commission of India, *Manual on Model Code of Conduct* (Mar. 2019), https://perma.cc/55KX-CW49.

[76] *Manual on Model Code of Conduct: About This File*, Election Commission of India, https://perma.cc/8E2R-3NGM.

[77] Election Commission of India, *Compendium of Instructions on Election Expenditure Monitoring* (Feb. 2019), https://perma.cc/Y54E-WNBA.

[78] Letter from ECI to Chief Electoral Officers et al., *Instructions of the Commission with respect to Use of Social Media in Election Campaigning*, Letter No. 491/SM/2013/Communication (Oct. 25, 2013), https://perma.cc/Z5VG-PPW9.

[79] Amogh Dhar Sharma, *How Far Can Political Parties in India Be Made Accountable for Their Digital Propaganda?*, Scroll.in (May 10, 2019), https://perma.cc/64VU-LDA5.

3. Information on Social Media Accounts

Rule 4A of the Conduct of Elections Rules, 1961, requires candidates or proposers of candidates to fill out an affidavit (Form 26) at the time of filing their nomination papers.[80] Paragraph 3 of this Form requires the candidate to provide the Commission with his/her "email ID" and a list of any social media accounts.[81]

4. Pre-Certification of Social Media content

The Election Commission requires pre-approval of political ads through "registration mechanisms for political advertisements on social media and have asked companies to establish grievance officers."[82]

On April 13, 2004, the Supreme Court of India issued an order requiring political parties, candidates, persons, "group of person of Trusts" to pre-certify or clear the use of political advertisements on electronic media, including television channels and cable operators.[83] Two days after the order, on April 15, 2004, the ECI issued detailed instructions on the matter:

> In this order, it was stated that every registered/national and State political party and every contesting candidate proposing to issue advertisements on television channels and/ or on cable network will have to apply to Election Commission of India/designated officer for pre-certification of all political advertisements on electronic media before the publication. The order was further modified and consolidated vide Commission's order dated 27.08.2012, wherein Media Certification and Monitoring Committees at district and State levels were given the responsibilities of pre-certification of such advertisement along with other functions viz acting against Paid News etc.[84]

In its 2013 instructions the Commission stated that, "[s]ince social media websites are also electronic media by definition," the Commission's instructions contained in its 2004 order "shall also apply mutatis mutandis to websites including social media websites and shall fall under the purview of pre-certification."[85]

---

[80] Conduct of Elections Rules, 1961, Rule 4A, https://perma.cc/DA6U-J5T8.

[81] Id., Form 26, para. 3, https://perma.cc/23XQ-QVZ4; *Instructions of the Commission with respect to Use of Social Media in Election Campaigning*, supra note 78.

[82] Sahana Udupa, Elonnai Hickok & Edward Anderson, *Can Extreme Speech Online Be Regulated Without Curbing Free Speech? This Series Finds Out*, Scroll.in (May 9, 2019), https://perma.cc/G6TS-8QLF.

[83] Letter from Election Commission of India to Chief Secretaries et al., *Supreme Court Order Dated 13th April, 2004 for Pre-certification of Political Advertisement on Electronic Media*, –Letter No. 491/MCMC/2018/Communication (Sept. 13, 2018) (re: applicability of 2004 directions throughout territory of India at all times), https://perma.cc/U2MM-U862.

[84] *Instructions of the Commission with respect to Use of Social Media in Election Campaigning*, supra note 78.

[85] Id.

The ECI establishes committees to prescreen political ads on social media for elections. According to one commentator "the efficacy of this exercise remains to be seen. Given the sheer size and dispersed nature of the platform, political advertisements found on the internet cannot be monitored with the same precision as those found on TV, newspapers, or radio." However, "in addition to technical difficulties in monitoring digital content," University of Oxford doctoral candidate Amogh Dhar Sharma notes other challenges including, first, "a political party's official social media and IT teams only represent a fraction of the organisational machinery through which political propaganda flows and circulates throughout the country" and "a large part of these activities also get outsourced to external agents whose services are hired by the party on a contractual basis. These services are often provided by political consultants, 'spin-doctors', and advertising firms."[86]

5. Transparency on Expenditure of Social Media Content

The Representation of the People Act, 1951, provides that every candidate is "required to keep a separate and correct account of all expenditure in connection with the election incurred or authorized by him or by his election agent between the date on which he has been nominatedand the date of declaration of the result thereof, both dates inclusive."[87] Following the 2014 Supreme Court of India decision in *Common Cause v. Union of India*,[88] the ECI required that political parties "submit a statement of expenditure of elections to the ECI and such statements are required to be submitted within 75 days of assembly elections and 90 days of Lok Sabha elections." In its 2013 instructions the ECI states that "social media is a part of all expenditure in connection with the elections" and that,

> [f]or the sake of removing any ambiguity, it is hereby directed that candidates and political parties shall include all expenditure on campaigning, including expenditure on advertisements on social media, both for maintaining a correct account of expenditure and for submitting the statement of expenditure. This, among other things, shall include payments made to internet companies and websites for carrying advertisements and also campaign related operational expenditure on making of creative development of content, operational expenditure on salaries and wages paid to the team of workers employed by such candidates and political parties to maintain their social media accounts, etc.[89]

III. Other Government Actions

A. Department for Promotion of Industry and Internal Trade

In late February 2019 the Government of India released a *Draft National e-Commerce Policy* from the Department for Promotion of Industry and Internal Trade which notes that online platforms

[86] Amogh Dhar Sharma, supra note 79.

[87] Representation of the People Act, 1951, § 77(1).

[88] Common Cause v. Union of India, Writ Petition (Civ.) No. 13 of 2003, https://perma.cc/G87R-JEYG.

[89] *Instructions of the Commission with respect to Use of Social Media in Election Campaigning*, supra note 78.

have a "responsibility and liability . . . to ensure genuineness of any information posted on their websites."[90]

B. Press Information Bureau of India

On April 2, 2018, "[n]oticing the increasing instances of fake news in various mediums including print and electronic media,"[91] the Press Information Bureau of India amended the *Guidelines for Accreditation of Journalists* to provide for the suspension of a journalist's accreditation for creating or propagating fake news under the following process:

> Now on receiving any complaints of such instances of fake news, the same would get referred to the Press Council of India (PCI) if it pertains to print media & to News Broadcasters Association (NBA) if it relates to electronic media, for determination of the news item being fake or not. Determination is expected to be completed within 15 days by these regulating agencies. Once the complaint is registered for determination of fake news, the correspondent/journalist whoever created and/or propagated the fake news will, if accredited, have the accreditation suspended till such time the determination regarding the fake news is made by the regulating agencies mentioned above. The Accreditation Committee of the PIB which consists of representative of both PCI and NBA shall be invariably be reached out to for validating any accreditation request of any news media agency. While any confirmation of publication or telecast of fake news having been confirmed by any of these agencies, the accreditation shall be suspended for a period of 6 months in the first violation and for one year in the case of 2nd violation and in the event of 3rd violation it would be cancelled permanently.[92]

However, the amendment was reportedly withdrawn soon after by the government because it "angered journalists and opposition politicians, who called it an attempt to gag the media in the run-up to national elections expected next year."[93]

IV. Media Coordination

In early 2019, leading up to the 2019 general elections, social media companies like Facebook, Twitter, and Google implemented more transparency measures for political advertisements on their platform and tools to deal with fake news.

A. Voluntary Code of Ethics

The Social Media Platforms (including Facebook, WhatsApp, Twitter, Google, ShareChat, TikTok, etc.) and the Internet and Mobile Association of India (IAMAI), an industry body, agreed

---

[90] *Draft National e-Commerce Policy: India's Data for India's Development* 29 (2019), https://perma.cc/C4H5-E86R.

[91] Press Release, Ministry of Information & Broadcasting, Guidelines for Accreditation of Journalists Amended to Regulate Fake News (Apr. 2, 2018), https://perma.cc/E3AH-ZBJT.

[92] Id.

[93] *India Withdraws Sweeping New Rule Clamping Down on Fake News*, Associated Press (Apr. 3, 2018), https://perma.cc/4ZSC-NP5D.

to a Voluntary Code of Ethics for the General Election 2019,[94] which went into effect on March 20, 2019, and remained in effect during the general elections.[95] The IAMAI highlighted that the purpose of the Code is to "identify the measures that Participants can put in place to increase confidence in the electoral process. This is to help safeguard the products and/ or services of the Participants against misuse to vitiate the free and fair character of the 2019 General Elections in India."[96] Social media companies agreed to implement the forty-eight-hour silence period of the Representation of the People Act on social media platforms and process reported violations within three hours, among other measures. Media Nama, a digital news portal, has provided a summary of what platforms have agreed to under the Code:

1. **Notification mechanism for ECI to report violations to platforms**: Platforms have developed a notification mechanism for the ECI to legally notify them of potential violations of Section 126 of the Representation of the People Act, 1951 and other electoral laws. The notification system for Google is a Google webform; a legal submissions portal page for Twitter; an email address for ShareChat and Facebook, per the Indian Express. Company officials said that they are yet to train the ECI on how to use their notification systems.
2. **Action within 3 hours for violations of 48-hour silent period**: For reported violations of Section 126 of the RP Act—which prohibits political parties and candidates from campaigning in the two days before voting—platforms will acknowledge and/or process these legal orders within 3 hours (as per the Sinha Committee recommendations). For other legal requests, platforms will act upon them "expeditiously" based on the nature of reported violation.
3. Platforms committed to "creating/opening a high priority dedicated reporting mechanism" for the ECI and "appoint dedicated person(s)/teams" during elections to contact and exchange feedback for acting upon legal requests from the ECI.
4. **Pre-certification for political advertisers**: The code requires platforms to provide a method for political advertisers to submit pre-certificates issued by ECI or its Media Certification & Monitoring Committee (MCMC) for running election-related ads. It requires that platforms "expeditiously" act on paid political ads which do not have a certification, as the ECI notifies. "Platforms will commit to facilitating transparency in paid political advertisements, including utilising their pre-existing labels/disclosure technology for such advertisements," states the code.
5. **Communication between the ECI, IAMAI, and platforms**: Platforms will update the ECI (via the IAMAI) on measures they have taken to prevent abuse of their platforms, pursuant to legal requests by the ECI. IAMAI will coordinate with platforms on the steps carried out under this Code, the industry body and the platforms will be in "constant communication" with the ECI during the election period. "Participants will deploy appropriate policies and processes to facilitate access to information regarding electoral matters on their products and/or services . . ." reads the code.
6. **Awareness and education campaigns**: The members will carry out information, education and communication campaigns to build awareness including electoral laws and other related instructions.

[94] Internet and Mobile Association of India (IAMAI), Voluntary Code of Ethics by the Social Media Platforms for the General Election 1-2 (2019), https://perma.cc/2NYR-8R3U.

[95] Press Release, Election Commission of India, Social Media Platforms Present "Voluntary Code of Ethics for the 2019 General Election" to Election Commission of India (Mar. 20, 2019), https://perma.cc/J2DU-HN23.

[96] IAMAI, supra note 94, at 1-2.

7. **Training nodal officers**: Platforms will train their nodal officers to the ECI on their products, and on the mechanism for sending requests to the platforms as per procedure established by law.[97]

B. Other Measures Taken by Social Media Platforms

Social Media and messaging platforms like Facebook, Twitter, WhatsApp, and Google have reportedly

> focused on bringing transparency to aspects of political content, verifying political advertisers, providing transparency in expenditure on political advertisements, more stringently monitoring content on their platforms, responding to government requests, including from the [ECI], raising awareness around disinformation and fake news, building capacity amongst politicians, and verifying content on their platforms.[98]

In February 2019, Facebook announced that it will carry disclaimer labels for political advertisements "offering details about those responsible for running the ad as the social media giant looks to bring transparency into political ads ahead of elections in India."[99] Also, Facebook has been blocking fake accounts and partnering with third-party fact-checkers for the elections.[100] Whatsapp has introduced a number of measures, according to one news source, including limiting "the number of times a user can forward a message to five. It also now labels forwarded messages."[101] The limits were reportedly introduced in July 2018

> after a spate of violence in early 2018, when rumors about child kidnappers, forwarded from person to person and group to group, fueled mass hysteria mainly in rural towns and villages across the country. In one incident in the state of Maharashtra, five people from a nomadic group were killed by a mob after rumors spread on the app about a child-abducting gang being active in the area. In all, at least 30 people were lynched in what came to be dubbed "WhatsApp Killings." In response, WhatsApp reduced the number of contacts or groups a user could forward a message to from 100 down to five in India, and 20 globally. (A WhatsApp spokesperson told TIME that during testing of the forwarding-limit, the company saw a 25% reduction of forwarded messages being shared.) In addition, WhatsApp added a "forwarded" label to passed-on messages.[102]

WhatsApp has also "introduced a fact-checking helpline, encouraging users to flag messages for verification. It also started re-circulating an old advertising video urging people to "share joy, not

---

[97] Trisha Jalan, *Social Media Platforms and IAMAI Enact 'Voluntary Code of Ethics' for Elections 2019; Some Challenges*, Medianama.com (Mar. 25, 2019), https://perma.cc/EV2A-P7KN.

[98] Elonnai Hickok, *To Address Extreme Online Content, Especially of the Political Kind, an Ecosystem Approach Is Needed*, Scroll.in (May 14, 2019), https://perma.cc/6TWX-XSDN.

[99] *Political Ads on Facebook to Carry Labels Offering Information on Advertiser*, The Hindu (Feb. 7, 2019), https://perma.cc/LUL9-8JAB.

[100] Phartiyal & Kalra, supra note 7.

[101] Ponniah, supra note 4.

[102] Billy Perrigo, *How Volunteers for India's Ruling Party Are Using WhatsApp to Fuel Fake News Ahead of Elections*, Time (Jan. 25, 2019), https://perma.cc/S8G2-7D4T.

rumors."[103] Leading up to India's recent general elections, Twitter launched a tool that lets users flag tweets that attempt to mislead voters.[104] However, according to one news report, "[t]hose policing social media content say steps being taken by social media giants to curb fake news are not even scratching the surface of the problem as false posts are shared faster than they can be taken down."[105]

[103] Rishabh R. Jain, *In India's Election, Voters Feed on 'Fake News' from Social Media, but Take It Seriously*, USA Today (Apr. 9, 2019), https://perma.cc/MJY2-27WF.

[104] Pranav Dixit, *Twitter Will Let Users Report Tweets that Mislead Voters*, BuzzFeed News (Apr. 24, 2019), https://perma.cc/P8BE-9U8Y.

[105] Pasricha, supra note 6.

Israel

Ruth Levush
Senior Foreign Law Specialist

SUMMARY Cybersecurity is viewed by the Israeli government as a vital national security interest due to geopolitical conditions. The fast pace of technological advances in cyberspace has caused particular concerns in recent years about the ability of external and internal actors to manipulate public opinion by spreading misinformation on social media and the impact of this development on democratic governance.

Specific concerns about foreign intervention in Israel's general elections were particularly highlighted ahead of the April 9, 2019, elections. Except for media reports on the hacking by Iranian intelligence of the cellphone of Benny Gantz, chair of the political alliance Kahol Lavan, no concrete data on cases of cyberattacks, dissemination of false information, or any other improper online behavior in connection with elections to the Knesset has been published.

Experts assert that while protecting critical infrastructure and organizations from cyberattacks is a challenge that is expected to be contained, the battle for public opinion created by the spread of misinformation requires a more complex treatment. The complexity of finding suitable legal measures derives from the need to balance the objective of protecting cyberspace with constitutional principles such as freedom of speech, the right to privacy, purity of elections, rules of transparency and parliamentary oversight of governmental activities, etc. An additional challenge to securing cyber systems is that regulation often lags behind the constant development of new technologies.

Several legislative proposals have been made to address cybersecurity and specific threats posed by the dissemination of misinformation. These include a bill regulating the mission, functions, and objectives of the Israel National Cyber Directorate and its authorities for the discovery and identification of cyberattacks against Israel, as well as warnings and information sharing about such attacks. Other bills specifically address transparency requirements for online political ads and the removal of foreign-financed and harmful online content. As of July 2019, these bills had not yet been adopted.

Although statutory transparency requirements in relation to election propaganda were originally limited to printed ads, the Central Election Committee (CEC) extended them to online election ads ahead of the April 9, 2019, national election. The CEC also recognized the duty of the government to refrain from publishing misleading information.

Prior to the April 9, 2019, election, Facebook blocked anonymous, paid Israeli political ads on its site, while Google blocked all advertising options related to segmentation, retargeting, and using a list of names by anyone engaged in political advertising.

Addressing the challenges of coping with fake news, the CEC for the upcoming September 17, 2019, national election has posted recommendations on identification of

misleading election-related information as well as contact information for reporting such information. The CEC has also posted video clips to clarify its message on this topic.

I. Background

Israeli governmental support for the development of cybersecurity is believed to be tied to the country's geopolitical conditions. Described as "a small community . . . under constant annihilation threat by other nations . . . [Israel has] developed creativity to compensate for its lack of resources."[1]

Cybersecurity policies and implementation apply to computerized systems as well as software applications and are handled at the national level by the Israel National Cyber Directorate (INCD), which reports directly to the Prime Minister.[2]

Cyber threats to Israeli targets may originate from both foreign and domestic sources. The ability to easily and speedily spread misinformation on social media, thereby manipulating public trust in national institutions or public opinion on other issues, is considered by Israeli decision makers and by experts as increasingly challenging. Addressing the spread of misinformation on social media by regulation, however, raises serious constitutional, institutional, and ethical concerns. This report addresses legal measures taken or proposed by Israeli legislators and policy makers, and evaluates their impact on basic principles of the Israeli legal system.

A. Concerns for Foreign Intervention Ahead of the April 9, 2019, Elections

According to Israeli media reports, the cell phone of Benny Gantz, chair of the political alliance Kahol Lavan, was hacked by Iranian intelligence prior to the April 2019 elections. Gantz was reportedly informed by Israel's General Security Service during the election campaign that his private device was breached and that the Iranians had the contents of his phone, including both personal and professional information. "Gantz was also informed that this served as a potential security risk, seeing as Iran might unveil information it finds on his cell phone after the election, or tamper with the election process."[3]

Specific concerns about the mass dissemination of misleading information by foreign and domestic players via social media were expressed in connection with the April 9, 2019, elections even before the finding of the cyber breach of Gantz's cell phone. According to Erez Kriner, former head of the Shin Bet Agency for Cybersecurity, there were several regional entities, in

[1] See Ben Ferguson, *How Israel Rules the World of Cyber Security*, VICE on HBO (June 13, 2019), https://video.vice.com/en_us/video/how-israel-rules-the-world-of-cyber-security/5a565b99177dd47339271be1 (forward to minute 3:00); see also Gill Press, *6 Reasons Israel Became a Cybersecurity Powerhouse Leading the $82 Billion Industry*, Forbes (July 18, 2017), https://perma.cc/XE9C-JQUV.

[2] Video, *Israel National Cyber Directorate*, gov.il, https://www.gov.il/en/departments/israel_national_cyber_directorate.

[3] *Israel Says Iran Hacked Ex-general Gantz's Phone Ahead of Election*, Haaretz (Mar. 14, 2019), https://perma.cc/J9XD-37DD?type=image.

addition to Russia, that might have been interested in influencing the Israeli elections: Turkey, Syria, Iran, the Palestinian Authority, and Hamas.[4] An Israeli cybersecurity company, however, estimated that Iran, Russia, and China posed the biggest threats, as they sought "to influence the outcome of elections or undermine confidence in the democratic process . . . [and] have the most money and people."[5]

A commentator opined that threats to the conduct of fair elections include voter data breaches, the hacking of party systems, and denial-of-service attacks on official sites:

> In the end, however, what might present the biggest threat comes from people trying to manipulate opinions by disseminating misleading information online; for example, by using fake Facebook profiles. . . . [T]he number of bots – fictitious social media users – could be enormous. Bots can be set up and maintained for three or four years and activated as an election gets underway. . . . The challenge is to maintain credibility and public trust in the process . . . . Sometimes it's enough to force down a government site for a few hours in order to instill public doubts about the cleanliness of the system.[6]

The Mossad (Israel's Secret Intelligence Service) Chief Tamir Pardo was quoted as saying "what we've seen so far with respect to bots and the distortion of information is just the tip of the iceberg. It is the greatest threat of recent years, and it threatens the basic values that we share—democracy and the world order created since World War Two."[7]

Except for the breach of security associated with the cell phone of Benny Gantz, no concrete data on cases of cyberattacks, dissemination of false information, or any other improper online behavior in connection with elections to the Knesset has yet been made available. Responding to a Knesset Information and Research Center (KIRC) request for such data, a representative of INCD reportedly noted that "the information is classified."[8] KIRC's report thus concluded that as of April 2019, the extent to which it was possible to retrieve data, and the ways to improve transparency without compromising aspects of data security and cyber security, appeared to be unclear.[9]

B. Spread of Misinformation by New Technologies

While protecting critical infrastructures or organizations from cyberattacks is a challenge that is expected to be contained, KIRC's report suggests that the battle for public opinion presents a

---

[4] Uri Berkowits, *"There Are At Least Four Countries in the Region that Will Be Interested in Influencing on the Elections in Israel,"* Globes (Jan. 10, 2019) (in Hebrew), https://perma.cc/ZX64-CJW5.

[5] Amitai Ziv, *Massive Manipulation, Foreign Influence Campaign and Cyber: The Threats to Israel's Election, What's behind the Shin Bet Chief Warning that a 'Foreign Country' Intends to Intervene in the Israeli Election*, Haaretz.com (Jan. 9, 2019), https://perma.cc/LE7Y-79SN?type=image.

[6] Id.

[7] Id.

[8] Roi Goldsmidt, KIRC, *Spreading False Information and Cyberattacks to Influence Elections* 7 (Apr. 2019) (in Hebrew), https://perma.cc/8N5K-FS2E.

[9] Id.

wider problem requiring more complex treatment as it may be conducted in cyberspace and is not limited to specific locations or directed at specific targets.[10]

Among technological tools that may be used in the battle for public opinion, experts have listed bots, big data, hacking, and trolls.[11] Bots may spread countless messages encouraging controversy, hatred, and violence in the form of posts or talkbacks for article published in online newspapers. The use of big data analysis allows for targeting specific audiences based on political preferences or perceived susceptibility for manipulation revealed by an individual's online record of activities on Facebook or other networks. Other means of possible online manipulation have included hacking legitimate accounts and the use of professional paid "talk backers" (trolls) and impersonating as innocent forums to recruit followers in order to prepare an infrastructure of followers for "command day".[12]

"Deepfake" is a new artificial intelligence-based technology that facilitates "joining 'deep learning' and 'fake news' [and] makes it possible to create audio and video of real people saying words they never spoke or things they never did."[13] Such technology may be used to create fear, perception of lack of control and harm to a person's privacy "in ways we have never thought of before." [14] In an op-ed published on the website of the Israel Democracy Institute (IDI) the authors opined as follows:

> The wider social implications of this technology are the main thing. This is not just a fear of fake imitation of political candidates. Deep-Fake technologies lead to an inability to distinguish between truth and lies; the growing difficulty in clarifying the reality and the phenomena and processes that take place in it; and our distrust of ourselves and our ability to find out what is right and wrong in the world around us. These three together threaten governmental bases, the functioning of institutions, and the ability to maintain functioning human and social relations. . . .
>
> As in other technological contexts, there are three ways to deal with the threat of Deep-Fake. The first way is to raise awareness of the public to identify fakes primarily by questioning. The problem is that sometimes the impact on people's awareness remains even after they realize that it is a forgery. More than that, teaching people not to believe anything involves heavy social costs.
>
> The second way is to create a cat-and-mouse race between Deep-Fake developers and those who develop identification technologies. . . .

[10] Id. at 3.

[11] Ron Shamir & Eli Becher, IDI, *Cyberattacks on the Election System- How to Compete?*, 136 Policy Research 31(Feb. 2019), https://perma.cc/XBW2-V9LU.

[12] Id. at 31-32.

[13] See, e.g., Dirk Kanngiesser, Commentary, *Toxic Data: How 'Deepfakes' Threaten Cybersecurity*, DARKReading (Dec. 27, 2018), https://perma.cc/Y2WC-L75Q.

[14] Tehila Schwartz Altshuler & Itay Baron, *Fake News: The Next Generation*, IDI (July 14, 2019) (in Hebrew), https://perma.cc/E4UV-BSD9.

> The third way is regulation, both for the development and distribution of Deep-Fake products. . . . [15]

The authors suggest that there may be a ground to distinguish between the regulation of fake news and deepfake, noting that,

> in the United States, social networks are exempt from responsibility for the content that passes through them, which is created to encourage the development of the internet. Social polarization, hate speech, and fake news have not yet caused the legislators to cancel the exemption, but Deep-Fake may be the watershed for imposing such responsibility. Not for nothing, Mark Zuckerberg said . . . that Facebook may treat Deep-Fake differently from fake news, which it refuses to touch.

To illustrate the challenge posed by the use of deepfake, the authors mention the case of "Deep-Nude," a deepfake application that allows creating nude images of women based on their images in dress, using a machine-learning algorithm. After half a million downloads and server crashes, the software was removed by its creator. In the authors' view,

> [t]he Deep Nude's story teaches once again that in technology itself, there is no need to do good and the challenge lies in setting moral boundaries. Recently, there have been voices that it is not enough to consider ethical considerations in the development of learning systems, but that that there are learning systems that need not be developed at all, even thru a legal prohibition, against all the difficulties that arise as a result. The Deep Nude software developer removed it from the servers, claiming that "the world is not ready yet." For that we can say, we are completely ready. We just do not want to [use it].[16]

The complexity of finding suitable legal measures for handling the spread of misinformation online appears, therefore, not only to reflect the challenge of finding the appropriate balance of such measures against constitutional and structural foundations of the legal system as discussed below, but also of catching up with the fast-paced development of new technologies, with the law sometimes lagging behind.

C. Constitutional Challenges Associated with Regulating the Spread of Misinformation

Experts have raised concerns regarding the impact of regulating the dissemination of information on the protection of free speech as well as on the right to privacy.[17] In addition, the regulation of cybersecurity at the national level may challenge principles of transparency, parliamentary oversight, and equality in elections, among others.

1. Freedom of Speech

A major challenge in regulating cyberspeech is how to balance it with the constitutional principle of freedom of speech. Israel's Supreme Court has recognized that protection of speech extends to

[15] Id. (all translations by author).

[16] Id.

[17] See, e.g., Shamir & Becher, supra note 11, at 11.

all forms of expression and all content of such expression, and encompasses freedom of the press and of political speech. It therefore extends to publications on social media. Freedom of speech, however, is not absolute and may be restricted under limited circumstances where there is "near certainty" that an expression would cause "real harm" to public safety. The right to freedom of speech may also be limited in circumstances where it conflicts with the right to human dignity, a right protected under Basic Law: Human Dignity and Freedom.[18] In addition, speech may be restricted based on statutory law containing prohibitions on incitement for racism, terrorism and violence, or denial of the Holocaust and praise for atrocities committed by the Nazis, or because it constitutes an insult to a public servant and defamation, among other limitations.[19]

In balancing freedom of speech against other principles recognized under the legal system, the courts have applied relevant balancing formulas. Recognizing the significance of protecting speech, the Supreme Court has applied a narrow interpretation to restrictions that may limit it, such as under the offense of insult to a public servant or defamation.[20] Recognizing a "defense of responsible journalism" against defamation suits, for example, the Court extended the defense, under appropriate conditions enumerated by law, to circumstances where the challenged publication was made in good faith, even if the information it contained ultimately turned out to be false.[21]

2. Democratic Principles of Transparency and Oversight

The concentration of cybersecurity authorities under a governmental body such as the INCD has been viewed as presenting challenges to democratic norms such as transparency and parliamentary oversight, among others.[22]

3. Principles of Fair and Free Elections

Specifically addressing the "institutional structure of the organizations that are responsible for various elements relating to the security of the electoral system . . . against cyber-attacks," an IDI article suggests as follows:

> The main problem lies in the fact that monitoring the internet in order to protect free and democratic elections is an activity that itself carries noticeable dangers for democracy, as there is a concern that tracking the activities of voters and of political activists may serve

[18] Basic Law: Human Dignity and Freedom, Sefer Ha-Hukkim [SH] 5752-1992 No. 1391, as amended, https://perma.cc/9CP2-X8K7.

[19] For additional information see Ruth Levush, *Initiatives to Counter Fake News in Selected Countries: Israel* 41 (Law Library of Congress, Apr. 2019), https://perma.cc/GPF9-RML4; Ruth Levush, *Limits on Freedom of Expression: Israel* 39 (Law Library of Congress, July 2019), https://perma.cc/UCL9-P23E.

[20] Additional Hearing, Crim 7383/08 Ungarfeld v. State of Israel (July 11, 2011) (in Hebrew), https://perma.cc/67CR-HPND.

[21] Additional Hearing Civil 2121/12 Anonymous v. Ilana Dayan, 67(1) Piske Din [PD] 667 (Sept. 18, 2014), https://perma.cc/87SA-FQ2Y; see also *Limits on Freedom of Expression*, supra note 19, at 44-45.

[22] See, e.g., Reference of the Israeli Internet Association (IIA) Regarding the Memorandum of the Cyber Protection Law and the National Cyber System (Aug. 9, 2019), https://perma.cc/KR6E-QTAQ (in Hebrew). See discussion in Part II(A), below.

> to limit freedom of expression and impinge on privacy and equality in the elections—interests that lie at the heart of the democratic process. Consequently the precondition for any regulation or legislation on this issue must be an assessment of its impact on freedom of expression, on privacy protections, and on other civil rights, given the particular sensitivity of the electoral process.
>
> Moreover, the extreme sensitivity of the electoral process requires unique rule of subordination and reporting, especially regarding the relation between the constitutional responsibility of the Central Elections Committee for the purity of the elections in their broadest sense, and the fact that the security organizations report directly to the government. It is also necessary to set principles for organizational coordination and boundaries regarding this issue between the security and enforcement agencies themselves, principles for notifying the public, and more.[23]

II. Current and Pending Legislation

A. Cybersecurity and National Cyber Directorate Bill

On December 27, 2018, the Knesset (Israel's parliament) passed the Law for the Regulation of Security in Public Bodies (Temporary Provision) (Amendment), 5779-2018 (Amendment Law).[24] The Amendment Law gives a statutory basis to the handling of cyberthreats and development of a national strategy by one organizational unit, the INCD.[25] The INCD incorporates the Israel National Cyber Bureau, which was initially established by an August 2011 government decision as a unit within the Prime Minister's Office. The Bureau had been tasked with promoting national preparedness for cyberdefense, including the formulation of a national defense concept in cyberspace and handling the protection of essential computer systems. The INCD website defines "essential computer systems" as those "the injury of which could cause significant physical or economic damage, harm to human life or damage to the provision of essential public service."[26]

Although recognized under the Regulation of Security in Public Bodies Law,[27] the INCD's mission, functions, and authorities are not yet regulated by law.[28] On June 20, 2018, the Israeli

---

[23] Shamir & Eli Becher, supra note 11, at vi-vii.

[24] Law for the Regulation of Security in Public Bodies (Temporary Provision) (Amendment), 5779-2018, SH 5779 No. 2766 p. 86, available at Reshumot, https://perma.cc/D5VL-XN44, amending the Regulation of Security in Public Bodies Law, 5758-1998, SH 5758 No. 1685 p. 348, as amended (both in Hebrew).

[25] Amendment Law § 2(3), amending section 1 of the Law; Amendment Law Draft Bill's Explanatory Notes, 5779-2018, Hatsaot Hok [HH] (Hamemshala) (government) Issue No. 1276 (Nov. 26, 2018) (in Hebrew). For information on the establishment and roles of the Israel National Cyber Directorate, see the Israel Government Portal (IGP), https://perma.cc/2WYV-GX3M.

[26] *Government Decisions and the Law for Regulating Security in Public Bodies*, INCD (July 16, 2018) (in Hebrew), https://perma.cc/Q7AE-MF55; see also Ruth Levush, *Israel: Law Recognizes Role of National Cyber Directorate in Protecting Cyberspace* (Law Library of Congress publication forthcoming).

[27] Security in Public Bodies Law, 5758-1998, SH 5758 No. 1685 p. 348, as amended.

[28] See Cyber Protection and the National Cyber Directorate Memorandum, 5778-2018 (Memorandum) (in Hebrew), https://perma.cc/46NY-C4Q5; see also *Summary of Memorandum of Cyber Protection Law (Summary)*, IGP (July 12, 2018) (in Hebrew), https://perma.cc/F79F-6E7R.

Prime Minister's Office published the Cyber Protection and National Cyber Directorate Memorandum, 5778. The Memorandum's stated objective is to propose the regulation of the mission, functions, and authorities of the INCD while implementing government policy in accordance with basic concepts of constitutional law and information technology. The bill proposed by the Memorandum would give the INCD the responsibility to establish a national technological infrastructure for discovery, identification, warning, and information sharing relating to cyberattacks against Israel.[29]

The Memorandum was distributed for public comment and was subjected to criticism by a number of experts, including the Israel Internet Association (IIA).[30] Among faults found in the Memorandum by the IIA were a lack of sufficient transparency; silence regarding the constitutional justification for the system of disclosure and identification; a lack of clarity regarding the relationship between provisions proposed in the Memorandum's draft bill to those in the Amendment Law; and faulty interface with criminal law enforcement agencies, such as the Israel Police. The IIA position is that the police force is a law enforcement body that deals mainly with civilians within the territory of the State of Israel. It should therefore be removed from the list of special bodies dealing with the defense of national security. The IIA further pointed to the silence of the Memorandum on the interaction between the INCD and other bodies that deal with issues related to cybersecurity and investigations that are likely to have an interface with issues defined in the Memorandum as a cyberthreat or cyberattack. Such bodies include the Authority for the Protection of Privacy, Israel Securities Authority, Antitrust Authority, the authority for Business and Fair Trade, etc.[31] The proposed legislation has not yet advanced.[32]

B. Transparency Requirement for Election Ads on the Internet

1. Committee for Examination of the Elections (Modes of Propaganda) Law

On July 8, 2015, Israel's President Reuven Rivlin and Justice Salim Joubran, the Chairman of the Central Elections Committee (CEC) for the 20th Knesset, appointed the Committee for Examination of the חוק הבחירות (דרכי תעמולה), תשי"ט- (Elections (Modes of Propaganda) Law, 5719-1959) (CEEMPL).[33] This Law governs the broadcasting of election messages in Israel.[34]

---

[29] Memorandum, supra note 28, at 3.

[30] See, e.g., Yaniv Kubovich, *Cyber Bill Would Give Netanyahu Unsupervised Powers, Experts Warn*, Haaretz (Mar. 19, 2019) (by subscription), https://perma.cc/X53L-MY2M.

[31] *Comments of the Israeli Internet Association (IIA) Regarding the Memorandum of the Cyber Protection Law and the National Cyber System*, Israel Internet Association (Aug. 9, 2019) (in Hebrew), https://perma.cc/TR9S-PKRD.

[32] For additional information on the INCD and Memorandum see *Israel: Law Recognizes Role of National Cyber Directorate in Protecting Cyberspace*, supra note 26.

[33] Elections (Modes of Propaganda) Law, 5719-1959, SH 5719 No. 284 p. 138, as amended; CEC, Appointment Letter Re: Committee for Examination of the Elections (Modes of Propaganda) Law, 5719-1959 (July 8, 2015) (in Hebrew), https://perma.cc/Q8H4-BFL4.

[34] Note that the word "propaganda" in Hebrew relates to election ads and does not necessarily have negative connotations, as it might in English. The term "propaganda" is being used in this report according to its Hebrew meaning and refers to political ads in general.

The CEC is established within sixty days of the convening of a new Knesset (Parliament) in accordance with the Knesset Elections Law.[35] The Committee is responsible for ensuring the proper conduct of elections and is headed by a Supreme Court justice elected by the panel of justices in the Supreme Court.[36]

The CEEMPL was established in response to past CEC chairs' recommendations to reform the Law and adjusts its provisions to reflect technological changes. The CEEMPL included the former President of the Supreme Court Dorit Beinish, former Minister of Justice Dan Meridor, former Knesset Member Itshak Levi, Professor Suzi Navot, and Professor Karin Nahon. The CEEMPL issued a comprehensive report and recommendations to the President on November 21, 2017.[37] The report stated that the Law was enacted in the pre-internet era.[38] It noted that the Supreme Court on a number of occasions has called for reformation of the Law in view of technological and telecommunications developments that have taken place over the years.[39]

One of the report's main recommendations was to extend the application of substantive provisions of the Law to the internet and to social platforms.[40] An additional recommendation was to add to the Law a special provision specifying as its objective the regulation of election propaganda, "[i]n fairness and transparency and in accordance with principles of freedom of expression, equal opportunity among candidates in elections and the dignity of men."[41]

A draft bill proposed by the CEEMPL clarified that transparency required disclosure of identifying information of the person, candidate, or candidates' list on behalf of whom the election advertisement was published, including on the internet.[42]

2. Bills Requiring Transparency

a. Elections (Modes of Propaganda) (Amendment No. 34) Bill, 5778-2018

Following the issuance of the CEEMPL report, the Knesset Constitution, Law and Justice Committee drafted the Elections (Modes of Propaganda) (Amendment No. 34) Bill, 5778-2018.[43]

---

[35] Knesset Elections Law [Consolidated Version] 5729-1969, SH 5729 No. 556 p. 103, as amended.

[36] Id. ch. D; see also *General Overview of the Committee and Its Activities*, CEC (in Hebrew), https://perma.cc/9MNE-VC85.

[37] Report of the Committee for Examination of the Elections (Modes of Propaganda) Law, 5719-1959 (5778-2017) (in Hebrew) https://perma.cc/86WN-KZTT.

[38] Id. at 6-7.

[39] Id. at 7-8.

[40] Id. at 15.

[41] Id. at 25.

[42] Proposed Text of Elections (Modes of Propaganda) Law (Consolidated Text of Existing Law with Committee's Recommendations), § 2A2, id. at 53 (this and other proposed bills in Hebrew).

[43] Elections (Modes of Propaganda) (Amendment No. 34), 5778-2018, HH (Knesset) No. 805 p. 273 (July 11, 2018), https://perma.cc/S6GH-NJU5.

The bill proposes, among other things, adding a section 2A1 to the Propaganda Law.[44] The proposed section would require an election ad to include the name and address of the person responsible for ordering it. If that person acted on the behalf of a competing person, party, or Knesset candidates' list, or on behalf of another body, the election ad would need to identify them.[45]

The bill defines "election ad" as either "election propaganda done by a person competing in the election, by a body connected to a party group, a body active in the elections or on their behalf,"[46] or as "the content of election propaganda that was written or disseminated for a fee."[47] For the purpose of transparency of the latter, a fee includes monetary and nonmonetary payment, provision of service, or any other benefit.[48]

According to the bill's explanatory notes, the distribution of any election ad, including on internet platforms and social media, is subject to the requirement of transparency. This requirement does not apply to ads circulated by individuals acting on their own who are not paid or who do not pay for writing or distributing the ads.[49]

Although the bill passed the first of the three readings required for adoption into legislation, no further progress has been made.[50]

b. Election Bill (Propaganda Methods) (Amendment – Prohibition of Financing Unidentified Propaganda) 5778-2018

A similar bill focusing on the transparency of election propaganda was proposed by six Knesset members on November 5, 2018.[51] This private members' draft bill does not appear to have yet been considered.[52]

[44] Id. § 5.

[45] Id., proposed section 2A1(a). For information on the election system see *Elections for the Knesset*, https://perma.cc/8L5L-CS7K.

[46] Elections (Modes of Propaganda) (Amendment No. 34), proposed section 2A1(b), § 5.

[47] Id.

[48] Id.

[49] Id., Explanatory Notes, at 275.

[50] Id., proposed section 2A 1(b).

[51] Elections (Modes of Propaganda) (Restricting Financing of Unidentified Propaganda) Draft Bill for Preliminary Reading, 5778-2018 (filed Nov. 5, 2018) (Unidentified Propaganda Bill), https://perma.cc/5PD8-FXWS.

[52] *Unidentified Propaganda Bill*, KNLD (in Hebrew), https://perma.cc/HB9D-L2PK

C. Removal of Content Found to Be in Violation of Law

1. A Bill to Prevent Foreign Propaganda

A private members' bill targeting propaganda directed by foreign countries was submitted on December 3, 2018, by three Knesset Members. According to explanatory notes to this bill, its intention was "to prevent advertising propaganda from abroad, or by corporations that are prohibited from donating to Knesset candidates' lists."[53]

The bill proposes to authorize the head of the CEC, who is a serving justice in the Supreme Court, to issue an injunction preventing the receipt of prohibited donations, monetary or otherwise, in accordance with the Parties Financing Law, 5733-1973.[54]

Similarly to the other "transparency bills," this bill has not yet been considered.[55]

2. Bills Proposing Removal of Online Harmful Content

Two additional bills were submitted to the Knesset in December 2016. The bills, dubbed "Facebook Laws," call for the removal of prohibited content from the internet. The first is a private members' bill that would require webmasters to remove from social platforms content that incites the commission of terrorist acts and impose fines on violators.[56] This bill had been incorporated into a government bill (the second of the two 2016 bills) that called for authorizing the Administrative Matters Court, under conditions enumerated by law, to issue a decree requiring the removal or disabling of the identification of content that constitutes a criminal act where there is a real possibility that continued publication would harm the safety of a person, public safety, or state security.[57]

A 2018 government bill called for facilitating, under relevant conditions, the issuance of content removal decrees within forty-eight hours from the filing of an application. It would have further authorize the issuance of decrees for the removal of content the publication of which constitutes a basis for the conviction of a person for an offense. The bill also called for authorizing consideration of inadmissible evidence in evaluating the merits of content removal requests

[53] Elections (Modes of Propaganda) (Amendment- Injunctions against Propaganda from a Foreign Country) Draft Bill for Preliminary Reading, 5779-2018 (filed Dec. 3, 2019) (Foreign Propaganda Bill), https://perma.cc/S5YM-9HLN.

[54] Id.; Political Parties (Financing) Law 5733-1973, SH 5733 No. 680 p. 52. For information on the financing of national elections in Israel see Ruth Levush, *Campaign Finance: Israel* (Law Library of Congress, Apr. 2009), https://perma.cc/9L63-BLF2.

[55] *Foreign Propaganda Bill*, KNLD (in Hebrew), https://perma.cc/GAJ6-TREG.

[56] Removal of Inciting Advertisement Published on a Social Network Platform, Bill, 5776-2016 (Private Members Draft Bill) (June 27, 2016), https://perma.cc/4GSB-RX8R.

[57] Removal from the Internet of Content the Publication of which Constitutes an Offence, Bill 5777-2016, HH (Government), Issue No. 1104 p. 741 (Dec. 28, 2016), https://perma.cc/2UM2-UC2T.

under certain circumstances.[58] Opponents of the bill argued that it constituted a threat to the democratic nature of the state, as it would violate freedom of expression and allow censorship to be imposed ex parte, and would be based on inadmissible evidence.[59] The government bill was reportedly withdrawn per Prime Minister Netanyahu's request.[60]

III. CEC Decisions

The CEC has issued several relevant determinations. It has clarified that the duty to prevent the spread of misinformation applies equally to the government as well as to individuals and bodies recognized by law. In addition, it has interpreted the duty to disclose the identity of issuers and publishers of content qualifying as election propaganda as also applying to online advertisers and online publishers.

A. Government's Duty to Distribute Accurate Information

A decision rendered on January 20, 2019, by Hanan Melcer, Deputy Supreme Court President and Chairman of the CEC, addressed the dissemination of misleading information by government institutions in the guise of election propaganda.[61] The case involved a petition filed with the CEC against Minister of Education Naftali Benet, who was a candidate in the April 2019 election, and the Ministry of Education requesting a halt to the dissemination of an allegedly false message produced by the Ministry asserting that the Minister has been successful in reducing classroom sizes throughout Israel during Benet's tenure.[62]

Accepting the petition, Melcer recognized that the message constituted "election propaganda" within the meaning of the Election (Modes of Propaganda) Law, and could not be produced or broadcast with public money.[63] Melcer's conclusion was based on an examination of the broadcast's "dominant objective" as reflected not only by the external circumstances of its publication, but also its substance:

> Therefore, the accuracy of the information presented in the publication, biased editing of material data, and omission of details, which may affect the messages presented in the publication, may also testify to the propaganda purpose which lies at the basis of the

[58] Prevention of Perpetrating Offenses by Publication on the Internet (Removal of Content) 5778-2018, Knesset Draft Bill (filed July 17, 2018), https://perma.cc/BX8A-2NPE.

[59] Omer Kabir, *The Law for Facebook Censorship in Israel Approved for Second and Third Reading*, Calcalist (July 15, 2018) (in Hebrew), https://perma.cc/24E4-3XBT.

[60] Moran Azulai, *Netanyahu Ordered to Stop Legislative Procedure for Enactment of "Facebook Law"*, ynet (July 18, 2018), https://perma.cc/5WF4-GWB7; see also Rafaela Goichman, *Facebook Law Returns: Arden Requests Netanyahu to Re-Promote the Bill*, The Marker (Dec. 4, 2018), https://perma.cc/8KT5-TDQJ (both in Hebrew).

[61] Election Case 3/21 Shahar Ben Meir v. Naftali Benet, Minister of Education et al., CEC for the 21 Knesset (Jan. 20, 2019) (in Hebrew), https://perma.cc/Y2YY-543Y.

[62] Id. ¶¶ 2-3.

[63] Id. ¶ 20.

> publication, and cast doubt on attempts to present it as useful [and] informative to the public.[64]

The broadcast of such a message, according to Melcer, violates the constitutional foundation for equality required in the Knesset elections process as it gives preference to the incumbent in relation to other candidates. This inequality, Melcer emphasized, was

> [r]einforced by the phenomenon of "false news" (Fake News), which has gained momentum in recent years. The need for publications to be accurate and devoid of any bias or political connotation, and this constitutes another reason for imposing a duty on the public authority to adhere to the truth and accuracy in every detail given on its behalf to the public.[65]

The fear of dissemination of false information, justifies, in Melcer's opinion, a sharpening of the guidelines and directives relating to government publications, to ensure that the "competent authority will fulfill its function only within the framework of its authority and will not obstruct public officials in activity in violation of . . . [election and government service laws]."[66]

Melcer held that any publication intended to be produced or disseminated by a controlled body (generally state and local governments and bodies receiving government funding) should be examined by its legal adviser for a determination of its accuracy and compliance with requirements under the Propaganda Law. Publications produced or disseminated in the absence of approval by the legal adviser will be deemed in violation of the prohibition on use of public assets in connection with an election under the Propaganda Law.[67]

The petition was accepted and the respondents were ordered to refrain from publishing the message and to remove it from any internet sites under their control. The Ministry was also ordered to remove the name of the Minister from any references to the Ministry's programs.[68]

B. Transparency Requirements of Online Election Ads ahead of April 2019 Elections

On February 27, 2019, Justice Hanan Melcer as Chairman of the CEC issued a decree, requiring identification of publishers of online propaganda on social networks and search engines. This requirement applied to all ads published by a party, a list of candidates, or anyone acting on their behalf. The objective of the decree was to increase transparency, improve ethical behavior, and prevent the unfair deception of voters.[69]

---

[64] Id. ¶ 29.

[65] Id. ¶ 30.

[66] Id. ¶ 32.

[67] Id.

[68] Id. ¶ 39.

[69] Press Release, Central Elections Committee for the 21st Knesset, An Innovative Order by the Chairman of the Elections Committee Indicates the Transparency of Online Propaganda (Feb. 27, 2019) (in Hebrew), https://perma.cc/2378-XYGY.

The decree specified that it applies to advertisers, and not to advertising platforms where advertising is done without editing or pagination, such as on Google or Facebook,

> [s]ince these platforms were not part of the process, and [they] made it clear that they would operate a mechanism of "notification and removal" so that citizens can report to platforms on propaganda publications and if it becomes apparent that the publication is anonymous, the platform will consider removing it. .[70]

The decision referenced in the above-cited decree accepted a petition that had been filed by two private attorneys against the Attorney General and ten parties and lists (blocs) of candidates that competed in the April 2019 national elections.[71] The petitioners requested an injunction ordering the respondents to refrain from publishing on the internet, on social media, and on other telecommunications platforms anything that might constitute election advertising, in the absence of identifying the party or list of candidates on behalf of which it is published.[72] Such disclosure is expressly mandated under section 10 of the Election (Modes of Propaganda) Law 5719-1959 (the Propaganda Law) for printed advertisements presented in public or by printed ads published in daily newspapers or magazines. Under this section,

> (a) Election propaganda shall not be made by means of printed advertisements presented in public, but by the following limitations:
>
> . . .
>
> (3) The ad shall bear the name and address of the printer who printed it and of the person responsible for ordering it; and if that person acted on behalf of a parliamentary group, [or] a list of candidates … the notice shall bear the name of the parliamentary group, [or] candidate list.
>
> . . .
>
> (b) Election propaganda shall not be made through printed ads published in daily newspapers or magazines, except with the following restrictions:
>
> . . .
>
> (5) The ad must bear the name and address of the person responsible for ordering it, and if the person acted on behalf of a party group, [or] a list of candidates … the notice shall bear the name of the parliamentary group, list of candidates, or the letter or alias of the faction or list of candidates.[73]

Stating that the limitations on election ads in cyberspace should be expressed in comprehensive legislation, Melcer nevertheless opined that the same limitations must be applied even in the absence of such legislation. In his opinion the limitations should be applied in a way that would reflect the objectives of the Law and balance them against the restrictions on freedom of political expression during the election period.[74]

---

[70] Id.

[71] Election Case 8/21 Shahar Ben Meir v. Likud Party et al., CEC for the 21st Knesset (in Hebrew), https://perma.cc/ZR7S-LR8H.

[72] Id. § 1.

[73] Election (Modes of Propaganda) Law 5719-1959, § 10(a)(3) & (b)(5), SH 5719 No. 284 p. 138, as amended.

[74] Election Case 8/21 ¶¶ 86–87.

Melcer recognized that in the new digital age, freedom of speech no longer applies to situations merely involving the speaker and the listener or viewer. Instead, it is "three-sided" in the sense that online platforms such as Facebook, Google, Twitter, WhatsApp, YouTube, Telegram, and other online publishers also play a role. Parties, lists of candidates, and similar bodies must adapt themselves to advertising on online platforms. Online publishers on their part also share responsibility to comply with relevant legal rules.[75]

Recognizing the need for transparency in response to national security concerns, Melcer further emphasized that

> [b]eyond legal liability – any anonymous advertising on the internet … makes it difficult for our security services to act to ward off fears of foreign interference in the upcoming elections to the 21st Knesset, which could be done in an anonymous manner, and this against the background of suspicions and lessons learned from election campaigns held in other countries in recent years.[76]

IV. CEC Information on Identification and Reporting of Misleading Information

On May 29, 2019, the 21st Knesset, which was elected on April 9, 2019, and sworn in on April 30, adopted legislation for its dissolution before the end of its term of office and for a new election to be held on September 17, 2019.[77]

To "maintain a fair, clean and truly democratic election process" the CEC for the 22nd Knesset posted a guide on its website titled *Coping with Fake News*.[78] Among recommendations for coping, the guide provides as follows:

> Fake News is often disseminated via "bots" and fake profiles. If you have, recently, received friend requests from unrecognized sources, check the following: When was the profile created? How many friends does this person have? Do you and they have any mutual friends? Another way to identify Fake News on social media is to ask yourself if the content is unique or if you have encountered it elsewhere. Also, Fake News is often poorly written, with spelling and grammatical errors and a low level of vocabulary and sentence structure. An interesting and useful experiment is to write to the source of the news item – and then check if the response is worded well, or if it feels like a poor, automated translation.
>
> . . .
>
> Social Media can be an excellent source of important information, but we must be attentive to the types of information and the sources we are being "fed." Always check if information is coming from a trustworthy and reliable source. The first clue is in the credits. Is the person sharing content which they themselves wrote, or are they sharing

[75] Id.

[76] Id. ¶ 87.

[77] Ruth Levush, *Israel: Legislation for Dissolution of Parliament and Holding a New Election Adopted* (Law Library of Congress, Apr. 2019), https://perma.cc/THH4-T455.

[78] *Coping with Fake News: Let's Keep This Election Campaign Clear of Fake News. Want to Know How? Read On, It's All in Here*, CEC, https://perma.cc/B72C-ZTKK.

> existing information which comes from other sources? Have they shared a lot of posts in a short amount of time? Are they a source of many types of information, or are they focused only on the upcoming elections? Does this source only share political postings? Is it all "scoops?" Is this source only involved in elections postings?[79]

The CEC website provides contact numbers for its service centers for all complaints and issues related to elections and voting. It further provides contact numbers for the police hotlines, as the police will also be responding to calls regarding computer crimes. Other reporting options include "the National Center for Cyber Incidents and Information Security . . . to complain about any attempts to manipulate voters through fake profiles and the like."[80] The CEC emphasizes that it does not send messages to or through social media, text messages, WhatsApp, etc.[81] Similar messages are conveyed in video clips linked through the CEC's Hebrew-language website.[82]

V. Media Coordination

A. Facebook's Blocking of Paid Election Ads and Fake News

According to Israeli media, Facebook announced that it would block anonymous, paid Israeli political ads on its site prior to the April 9, 2019, Knesset election. According to its new policy, "advertisers on Facebook will be required to provide a verified local contact person and disclosure [sic] what was paid for the ad and by whom."[83] Facebook's commitment to block anonymous ads was expected to address the fraudulent depiction of political parties' sponsored ads in the guise of private ads.[84]

In a January 31, 2019, press release, Facebook announced that it had

> [r]emoved 783 Pages, groups and accounts for engaging in coordinated inauthentic behavior tied to Iran. There were multiple sets of activity, each localized for a specific country or region, including . . . Israel . . . . The Page administrators and account owners typically represented themselves as locals, often using fake accounts, and posted news stories on current events. This included commentary that repurposed Iranian state media's reporting on topics like Israel-Palestine relations.[85]

---

[79] Id.

[80] Id.

[81] Id.

[82] *Stop Believing Fake News*, YouTube (Mar. 21, 2019) (in Hebrew), https://youtu.be/vgfmx73mNuM; *Don't Give a Hand to Fake News*, YouTube (Mar. 27, 2019) (in Hebrew), https://youtu.be/IJWcCuOH5IQ.

[83] Chaim Levinson, *Facebook to Block Anonymous Paid Political Ads before Israel's Election*, Haaretz (Jan. 28, 2019), https://perma.cc/BB3S-ARRZ.

[84] *Id.*

[85] *Removing Coordinated Inauthentic Behavior from Iran*, Facebook Newsroom (Jan. 31, 2019), https://perma.cc/K2HX-D4CE.

B. Google's Blocking of Personalized Advertising During the 2019 Election Period

Google reportedly informed Israeli media companies in early February 2019 that they would not be able to execute personal advertising on the company's systems until after the April 9 elections. This means that Google would block all advertising options related to segmentation (advertising to a segmented audience), retargeting, and using a list of names to anyone engaged in political advertising.[86]

[86] Anat Bain Lubobitz, *Google's Dramatic Decision – Stops Personalized Advertising during Election Time*, Globes (Feb. 7, 2019) (in Hebrew), https://perma.cc/75FT-EW2P.

Mexico

Gustavo Guerra
Senior Foreign Law Specialist

SUMMARY Mexico does not currently have legislation specifically addressing the issue of misinformation disseminated through social media in the context of elections. Instead, this issue has been addressed by election authorities through information campaigns against "fake news." These efforts have been supported by social media companies through collaboration agreements with the Mexican government. News organizations also launched a campaign known as "Verificado" ("Verified") aimed at vetting news concerning the 2018 national elections.

I. Background

Mexican authorities recognize disinformation through social media as a serious issue but have not enacted specific legislation on the topic.[1] Rather, they are countering disinformation with official information.[2]

The head of Mexico's National Institute of Elections (INE) has stated that social media sites present a number of challenges that potentially could have an impact on elections, given the volatility of information presented on such sites and the ease with which images and news aimed at promoting or attacking political parties and candidates can be distorted.[3] He has also indicated that the INE responds to misinformation with truthful information on elections disseminated through social media platforms instead of trying to censor, limit, or punish the use of social media for misinformation purposes, in an effort to assist the public in making informed decisions concerning elections.[4]

Mexico's Constitution provides that, generally, the expression of ideas may not be subject to any administrative or judicial inquiries, although this general principle is limited by certain exceptions, such as when expressing those ideas may cause the commission of crimes or disturb public order.[5] The Constitution also provides that all individuals have the right to disseminate

[1] Tribunal Electoral del Poder Judicial de la Federación, Recurso De Revisión Del Procedimiento Especial Sancionador Expediente: SUP-REP-143/2018, Aug. 23, 2018, at 31, https://perma.cc/XW6H-A6E9.

[2] Instituto Nacional Electoral (INE), *La desinformación que afecta a la democracia, debe combatirse con mecanismos democráticos y no con censura: Lorenzo Córdova*, Central Electoral (Apr. 25, 2019), https://perma.cc/K5T7-2EXB.

[3] Id.

[4] INE, *Presenta INE modelo de combate a la desinformación en elecciones 2018-2019*, Central Electoral (July 18, 2019), https://perma.cc/WYS8-E3D2.

[5] Constitución Política de los Estados Unidos Mexicanos art. 6, Diario Oficial de la Federación [D.O.F.], Feb. 5, 1917, as amended through 2019, https://perma.cc/C8KD-ZKED.

information and ideas through any communication medium,[6] subject to an exception for election-related libel, discussed below.

II. Current and Pending Legislation

As noted, Mexico has not enacted legislation that specifically addresses the issue of misinformation disseminated through social media in the context of elections,[7] and no pending legislation on the topic was identified. However, the Constitution provides that political parties and candidates must refrain from committing libel through political advertisements during elections.[8] Mexico's Elections Court has ruled that this type of libel may be committed through social media.[9]

III. Other Government Actions

The INE signed collaboration agreements with Facebook and Google concerning news about Mexico's 2018 national elections.[10] The agreement with Facebook provided for workshops aimed at training relevant INE staff on how to use this social medium as well as best practices on political communications on the platform.[11] Furthermore, the INE was to disseminate to the public informational materials developed by Facebook and civic organizations that contained guidelines on detecting low-quality content available on the internet, thus assisting the public in being able to identify trustworthy information.[12]

The agreement with Google provided for Google to assist the INE in disseminating official information on the 2018 elections, including information on how to vote per applicable requirements, locating voting places in Google maps, and broadcasting presidential debates live on Google subsidiary YouTube.[13]

IV. Media Coordination

In addition to the collaboration agreements discussed above, more than sixty media companies and nongovernmental organizations launched an online effort called "Verificado" (roughly translated as "Verified") to monitor the veracity of news pertaining to the 2018 Mexican

[6] Id.

[7] Tribunal Electoral del Poder Judicial de la Federación, supra note 1, at 31.

[8] Constitución Política de los Estados Unidos Mexicanos art. 41-III(C).

[9] Tribunal Electoral del Poder Judicial de la Federación, supra note 1, at 34, 35.

[10] INE, *Presenta INE modelo de combate a la desinformación en elecciones 2018-2019*, supra note 4.

[11] INE, *Facebook e INE anuncian colaboración para elecciones*, Central Electoral (Feb. 5, 2018), https://perma.cc/LE3L-RTH6.

[12] Id.

[13] INE, *Colaboran INE y Google para mantener informada a la ciudadanía sobre el Proceso Electoral*, Central Electoral (Apr. 8, 2018), https://perma.cc/45BF-B28M.

elections.[14] Sponsors included Facebook, Google News Lab, Twitter, Open Society, and Oxfam.[15] Verificado also opened Twitter and Facebook accounts in order to disseminate news previously vetted by its team of researchers as well as to explain to the public the falsity or inaccuracy of election information circulated online when appropriate.[16] The vetting process ranged from fact-checking of partially inaccurate information through declaring it "fake news," as necessary.[17]

[14] *¿Qué es Verificado 2018?*, Verificado 2018, https://perma.cc/RAP9-3UZD.

[15] Id.

[16] Id.

[17] Id.; *Así funciona #Verificado2018 – Metodología*, Verificado 2018, https://perma.cc/7M6D-C5R9.

Russian Federation

Astghik Grigoryan
Legal Research Analyst

SUMMARY The Government of the Russian Federation considers information security an integral part of national security. Two key documents, the Information Security Doctrine and the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030, set priorities for information security, and identify major threats and ways to counter them.

The Constitution of the Russian Federation contains free speech guarantees, and varied aspects of information accuracy, including election campaign information, are regulated by federal laws, such as the Law on Information, Mass Media Law, and the Law on Basic Guarantees of Voting Rights.

Recently adopted legislation restricts access to information containing fake news or insults and disrespectful messages related to the symbols of the Russian Federation, the Constitution, and the authorities. Spreading banned information is punishable by fines and administrative detention. The Criminal Code of the Russian Federation contains articles prescribing various punishments for spreading defamatory content. Measures to remove banned content and limit access to websites containing restricted information were introduced in 2019.

The Russian government is planning to create an open registry of fake news sites, with identification of the platforms and their respective authors. The registry will be accessible to the public. The Russian legislature's lower chamber is planning an examination of news aggregators with an aim of controlling the distribution of fake news and disinformation. So far, Spain is the only country with which the Russian government has signed a cybersecurity agreement, to counter the impact of disinformation on diplomatic relations between the two nations.

Russian media organizations are critical of the adoption of anti-fake-news laws, viewing these laws as overly restrictive and arbitrary.

I. Background

The internet and social media are widely available and accessible to a large segment of the Russian population. According to the statistical website Statista, the number of internet users in Russia has been growing steadily in the past six years, reaching one hundred million users in 2019.[1] According to the same source, the majority of the Russian population uses social media. As of 2017, the most popular social media networks in the Russian Federation were YouTube (68%) and VKontakte (61%).[2]

[1] *Number of Internet Users in Russia from 2013 to 2019 (in Millions)*, Statista, https://perma.cc/NS4X-ZE3X.

[2] *Penetration of Leading Social Networks in Russia as of 4th Quarter 2017*, Statista, https://perma.cc/JCB4-9PXJ.

For the Government of the Russian Federation, information security is an indivisible component of overall national security. The government's Doctrine of Information Security[3] emphasizes the importance of regulating the internet within the borders of the Russian Federation and recognizes as a security threat all content that contains extremist ideology, spreads xenophobia, or promotes violent change to the constitutional order or a violation of the Russian Federation's territorial integrity.[4]

Based on the principles and priorities outlined in the Doctrine, Russia adopted the Strategy for the Development of an Information Society in the Russian Federation for 2017–2030.[5] One of the Strategy's declared goals is "the creation of a safe information environment based on information resources that contribute to the spread of traditional Russian spiritual and moral values."[6] To achieve this goal, amendments are foreseen to legal, regulatory, and technological systems aimed at the protection of the information sphere in Russia by blocking access to banned resources and removing them.[7] Recently adopted changes in legal regulation of the media address such means of accessing information as internet TV, news aggregators, social networks, internet sites, and instant messaging.[8]

II. Constitutional Protection of Free Speech

Article 29 of the Constitution of the Russian Federation contains free speech guarantees, as well as the right to freely search, receive, and disseminate information by legal means.[9] The Constitution bans any kind of censorship.[10]

Constitutional guarantees of free speech do not apply, however, to "hate speech" or propaganda asserting social, racial, national, religious, or linguistic supremacy.[11] Article 55 of the Constitution states that

> [t]he rights and freedoms of man and citizen may be limited by the federal law only to such an extent to which it is necessary for the protection of the fundamental principles of

[3] Resolution of the President of the Russian Federation on Approving Information Security Doctrine (Dec. 5, 2016) (in Russian), https://perma.cc/4BEK-4M5R.

[4] Id.

[5] Decree of the President of the Russian Federation on the Strategy for the Development of an Information Society in the Russian Federation for 2017-2030, N 203 (May 9, 2017), http://pravo.gov.ru (official legal information portal) (in Russian), https://perma.cc/AQ4H-CE79.

[6] Id. § 26.d.

[7] Id. § 26.o.

[8] Id. § 26.p.

[9] Constitution of the Russian Federation (1993) art. 29, https://perma.cc/RZ7Y-EBFA.

[10] Id.

[11] Id.

> the constitutional system, morality, health, the rights and lawful interests of other people, for ensuring defense of the country and security of the State.[12]

The Russian Federation ratified the European Convention on Human Rights in 1998.[13] Article 10 of the Convention guarantees freedom of speech.

III. Current Legislation

The Federal Law on Information, Information Technologies, and the Protection of Information (Information Law) is the main legislation in the information management field and prescribes legal standards for the search, production, transfer, and dissemination of information.[14] The Information Law was amended in 2017 with provisions that restrict access to information resources that are banned within the territory of the Russian Federation.[15] In March 2019, Russia adopted two so-called anti-fake-news laws, which amend the Information Law with provisions establishing the procedure for deleting information recognized as false and prescribing punitive measures for disseminating fake news.[16] At the same time, the Information Law and the Code of Administrative Violations were amended by laws prohibiting the online publication of content that disrespects state symbols, the Constitution, and Russian Federation authorities.[17]

Certain provisions of the Criminal Code prescribe punishments for the distribution of inaccurate, defamatory, and false content.

Information coverage of elections and referenda is regulated by the Federal Law on Basic Guarantees of Voting Rights and the Right to Participate in a Referendum of Citizens of the Russian Federation (Voting Rights and Referendum Law).[18] Chapter VII of the law regulates the dissemination of election ads.[19] The law does not contain specific provisions concerning

---

[12] Id. art. 55.

[13] European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms (1950), https://perma.cc/RRM2-LVG6.

[14] Federal Law on Information, Information Technologies, and Protection of Information (Information Law), No. 149-FZ (July 27, 2006) (in Russian), https://perma.cc/86PF-DYTH.

[15] Federal Law on Amendments to the Information Law, No. 276-FZ (July 29, 2017) (in Russian), https://perma.cc/V4GW-MGJA.

[16] Federal Law on Amending Article 15-3 of the Federal Law on Information, Information Technologies, and Protection of Information (Law on Amending Article 15-3 of the Information Law), No. 31-FZ (Mar. 18, 2019) (in Russian), https://perma.cc/7YEP-QHU8; Federal Law on Amending the Code of Administrative Violations, No. 27-FZ (Mar. 18, 2019) (in Russian), https://perma.cc/E3CL-H6KM.

[17] Federal Law on Amending the Federal Law on Information, Information Technologies, and Protection of Information (Law on Amending the Information Law), No. 30-FZ (Mar. 18, 2019) (in Russian), https://perma.cc/HCG6-6ZBC; Federal Law on Amending the Code of Administrative Violations, No. 28-FZ (Mar. 18, 2019) (in Russian), https://perma.cc/Z6N8-UW62.

[18] Federal Law on Basic Guarantees of Voting Rights and the Right to Participate in a Referendum of Citizens of the Russian Federation (Voting Rights and Referendum Law), No. 67-FZ (June 12, 2002), as amended (in Russian), https://perma.cc/N4HJ-SP5E.

[19] Id. ch. VII.

distribution and accuracy of election ads on social media. Provisions of the law apply to audiovisual and print media as well as to ads distributed via the internet.

The Law on Mass Media also contains provisions pertaining to the regulation of media during election campaigns and referenda that are similar to those of the Voting Rights and Referendum Law.[20]

A. Information Law

The Information Law contains provisions aimed at countering the dissemination of inaccurate or untrue information.[21] Article 3, paragraph 6 of the law declares ensuring the reliability and trustworthiness of the information one of its major principles.[22]

The law guarantees freedom of dissemination of information unless it is aimed at "propaganda of war, [or] incitement of national, racial, or religious hatred and enmity, as well as other information for the dissemination of which criminal or administrative responsibility is provided."[23]

The law imposes additional trustworthiness requirements on the news distributed through a news aggregator. The owner of the aggregator (only Russian physical or legal persons can own news aggregators) must be responsible for verifying the validity of socially significant facts, as well as preventing the use of the news aggregator to conceal or falsify socially significant information and disseminate false socially significant news information under the guise of reliable messages.[24]

If falsification of socially significant information (including the distribution of unreliable information of social significance under the guise of reliable messages) is found on the news aggregator, the authorities have the right to apply to Roskomnadzor, the federal executive body overseeing mass media and information technology, to take necessary measures to stop the distribution of such disinformation.[25]

If information is distributed illegally, the Prosecutor General of the Russian Federation or the prosecutor's deputies may petition Roskomnadzor to stop the distribution of such information.[26]

---

[20] Federal Law on Mass Media, No. FZ-2124-I (Dec. 27, 1991), as amended (in Russian), https://perma.cc/MCH9-UT53.

[21] Information Law arts. 3, 15-3.

[22] Information Law art. 3, para. 6.

[23] Id. art. 10.

[24] Id. art. 10(4), paras. 2, 3, 12.

[25] Id. para. 8.

[26] Id. art. 15.3.

B. Anti-Fake-News Laws

1. Overview

Amendments to the Information Law of March 2019 defined fake news as "socially significant" false information distributed under the guise of truthful messages that endanger people's lives, health, or property; create possibilities for mass violations of public order or public security; or could interfere with transportation, social infrastructure, credit institutions, modes of communication or industry and energy enterprises.[27]

The law authorizes the Prosecutor General's office to determine whether information is false or not and define the degree of harm inflicted by distribution of false information.[28] The latter forwards to Roskomnadzor a request to take measures limiting access to untrustworthy information.[29]

The Law on Amending Article 15-3 of the Information Law specifically provides for control over the distribution of fake news in online media. It states that Roskomnadzor is to inform the editorial body of an online publication concerning the removal of fake news. Upon receipt of a notice from Roskomnadzor, the editorial body must immediately take steps to remove such information and, if it fails to do so, Roskomnadzor must take steps to limit access to the online publication. In such cases, the internet service provider must also immediately block access to the sites where the fake news is published.[30]

The Law on Amending the Code of Administrative Violations prescribes the following punishments for spreading fake news:

- Complicit citizens: Fined from 30,000 to 100,000 rubles (approximately US$458 to $1,528). For repeat violations, the fines range from 100,000 to 300,000 rubles (approximately US$1,528 to $4,580).
- Complicit officials: Fined from 60,000 to 200,000 thousand rubles (approximately US$916 to $3,000). For repeat violations, the fines range from 300,000 to 600,000 rubles (approximately US$4,580 to $9,100).
- Complicit legal persons: Fined from 200,000 to 500,000 rubles (approximately US$3,000 to $7,600) and confiscation of offending tools. For repeat violations, the fines range from 500,000 to 1 million rubles.[31]

Should the dissemination of fake information cause the "death of a person or harm to human health or property, a massive disturbance of public order and (or) public safety, the cessation of the functioning of life support facilities, transport or social infrastructure, communications, credit institutions, energy or industry," the fines range as follows:

---

[27] Information Law art. 15-3, § 1.1.

[28] *What Is Fake News and What Punishment Does Spreading It Entail?,* State Duma (in Russian), https://perma.cc/G5D2-9LGC.

[29] Id.

[30] Law on Amending Article 15-3 of the Information Law arts. 1.1-1.4.

[31] Law on Amending the Code of Administrative Violations art. 1, § 4.

- Complicit citizens: Fined from 300,000 to 400,000 rubles (approximately US$4,580 $6,100).
- Complicit officials: Fined from 600,000 to 900,000 rubles (approximately US$9,100 to $13,700).
- Complicit legal entities: Fined from 1 million to 1.5 million rubles (approximately US$15,270 to $22,900).

Repeat offenders may also be subject to up to fifteen days' administrative arrest.[32]

2. Litigation

The first lawsuit challenging the provisions of the anti-fake-news laws was brought in the city of Arkhangelsk. The defendant was a Russian political activist, Elena Kalinina, who publicized a protest against the selection of a site in Arkhangelsk for waste disposal on her social media (VKontakte) account. The authorities charged that Kalinina was aware the protest in question was not sanctioned and could not take place legally, so publicizing it amounted to spreading disinformation. Kalinina's attorney asserted that the lawsuit infringed the activist's constitutional right to "freely receive and disseminate information."[33] The court dismissed the case, stating that the charges brought by police did not specify which words were false in particular, what made them false, and under what criteria the police determined that false information was disguised as true.[34] The court said the presence of all these elements is required in order to qualify a news publication as fake. The court also stated that violating the procedure for organizing a public event or publicizing an unauthorized event is not a violation of the anti-fake-news law.[35]

C. Laws Prohibiting Publication of Content Disrespectful to State Symbols, the Constitution, and the Authorities

Procedures similar to those that ban the distribution of fake news are prescribed for blocking access to content "that offends human dignity and public morality, [or shows] obvious disrespect for society, the state, official state symbols of the Russian Federation, the Constitution of the Russian Federation, or authorities exercising state power in the Russian Federation."[36]

Upon discovery of such content, the Prosecutor General must forward to Roskomnadzor a motion to remove it and to restrict access to information resources that disseminate it. Roskomnadzor, based on the prosecutorial motion, must immediately determine which internet access providers are hosting the content and send electronic notifications (in both English and Russian) identifying the domain name and network address with a demand to remove it. The providers must contact the content's owner, which must remove it within one

[32] Id.

[33] *Human Rights Activists Announced the First Case under the Law on Fake News*, RBC (Apr. 29, 2019) (in Russian), https://perma.cc/8CVB-UJAY.

[34] *The Court Refused to Review a Case under Anti-Fake News Law*, 29.ru (May 23, 2019) (in Russian), https://perma.cc/ZRY7-8T28.

[35] Id.

[36] Law on Amending the Information Law, No. 30-FZ (Mar. 18, 2019), art. 15^{1-1}, § 1.

day. If the owner does not comply, Roskomnadzor must direct the providers to block access to the website. The banned content's owner must inform Roskomnadzor when the content is removed. After Roskomnadzor verifies that the content was removed, it directs telecommunication companies to restore access to the site.[37]

Spreading banned information is punishable by a fine or administrative arrest. The following punishments are prescribed by the law: for a first-time violation, 30,000 to 100,000 rubles (approximately US$458 to $1,528); for repeat offenses, from 100,000 rubles (approximately $1,528) up to fifteen days of administrative arrest. If a person has committed violations two or more times, the punishment will range from 200,000 rubles (approximately $3,000) to fifteen days of administrative arrest.[38]

D. Criminal Code

Defamation is punished under the provisions of the Criminal Code. The Code defines defamation as the "dissemination of knowingly false information, discrediting the honor and dignity of another person or undermining his reputation,"[39] and stipulates different punishments (monetary, compulsory public works, or imprisonment) based on its impact. Specifically, article 128.1(2) states that "libel contained in a public statement, a publicly displayed work, or the media is punishable with a fine of up to 1 million rubles [approximately US$15,000] or an amount equal to the salary or other income of the convicted person for a period of up to one year, or compulsory work for a period of up to 240 hours."[40]

Stricter punishments (including higher fees and compulsory public works) are provided for in the Criminal Code for the defamation of persons involved in the administration of justice, including judges, jurors, prosecutors, investigators, and bailiffs.[41]

E. Federal Law No. 276-FZ on Amendments to the Information Law

Federal Law No. 276-FZ amended the Information Law to prohibit providing access to information resources or internet sites that are banned within the territory of the Russian Federation.[42] The amending law authorizes Roskomnadzor to create and maintain a state registry of information resources with limited access in Russia.[43] Roskomnadzor must also ensure that investigative bodies have full access to the hardware and software of resource providers, and the law authorizes Roskomnadzor to require that a provider fully identify the owner of its hardware and software. The provider must comply with the demand within three

[37] Id.

[38] Federal Law on Amending the Code of Administrative Violations, No. 28-FZ, art. 1, § 2.

[39] Criminal Code of the Russian Federation, as amended, art. 128.1 (June 5, 1996) (in Russian), https://perma.cc/ APZ9-5MZ8.

[40] Id. (translation by the author).

[41] Id. art. 298.1.

[42] Federal Law on Amendments to the Information Law, No. 276-FZ (July 29, 2017), note 19.

[43] Id. art. 3, § 2.1.

working days. The name of the owner of the resources must be entered into the state registry of information resources with restricted access within thirty working days, as well as the name of any operators of advertisement search engines connected to the site.[44] The amending law obligates owners to limit access to banned resources within three days after inclusion in the federal registry;[45] Roskomnadzor must instruct telecommunications companies to block providers' access within twenty-four hours if they fail to comply.[46]

F. Voting Rights and Referendum Law

1. Overview

The Voting Rights and Referendum Law states that supporting information for a referendum includes the provision of information and propaganda to voters and referendum participants.[47] It also provides that "[t]he content of information materials posted in the media or distributed in another way must be objective, reliable, and must not violate the equality of candidates and (or) electoral associations."[48] The law stipulates that information about ongoing election- and referendum-related events should be published exclusively as a separate "information block," without editorial comment. These information blocks must not be paid for by candidates, electoral associations, or referendum initiative groups, and should not give preference to "any candidate, electoral association, referendum initiative group, [or] other group of referendum participants." The law also prohibits any discrimination regarding coverage time and allocation of print space.[49] The candidates are free to choose broadcast media and the content of their election ads.[50]

The law regulates publication of public opinion poll results. In particular, it stipulates that a publisher must provide information regarding the methodology of a poll, identify the organization in charge of polling, specify the surveyed area, number of respondents, and questions asked, and identify who paid for publication of the poll results.[51] With certain exceptions, it also stipulates that publishing a person's photograph and citing his or her opinion in election ads for a referendum requires that person's prior written approval.[52]

[44] Id. art. 3, §§ 2.4, 5.

[45] Id. art. 3, § 7.

[46] Id.

[47] Voting Rights and Referendum Law art. 44, note 22.

[48] Id. art. 45, § 2.

[49] Id. art. 45, § 5.

[50] Id. art. 48.

[51] Id. art. 46.

[52] Id. art. 48.

Election ads can be paid for by the candidates' election funds or by the state. When ads are placed in non-state-owned media, the owner of the media organization must announce the conditions for placing such ads. Parity among candidates in time allocation and rates for these ads is required.[53]

2. Limitations on Provision of Information during Election Campaigns

The campaign period in an election starts twenty-eight days before election day and ends at midnight on the day before election day.[54] Campaigning and providing information on voting results on election day are prohibited,[55] as is the dissemination of public opinion poll results starting five days before election day.[56]

The law prohibits publishing content, including online ads, that incites "social, racial, national or religious hatred, degrades national dignity, [or] promotes exclusivity, superiority or inferiority of citizens on the basis of their attitude to religion, social, racial, national, religious or linguistic affiliation."[57]

If mass media entities publish an election ad that contains content (including reliable information) that could damage the honor, dignity, or business reputation of a candidate, they must also publish the candidate's response, giving the response equal time and prominence.[58]

The law prohibits federal, state, and local governments from informing voters about candidates or electoral associations.[59]

G. Mass Media Law

According to the Law on Mass Media, people must be allowed to search, receive, produce, and distribute mass information without restriction.[60] Article 2 of the law was amended in 2011 to include "network publication," which is defined as an internet site legally registered as a media outlet.[61] While the law bans censorship,[62] using mass media to disclose state secrets or privileged information, or to disseminate information containing "hate speech" or inciting terrorism, is

[53] Id. art. 50, § 5.

[54] Id. art. 49, § 2.

[55] Id. art. 45.

[56] Id. arts. 45 & 49, § 3.

[57] Id. art. 56, § 6.

[58] Id. art. 56.

[59] Id. art. 45.

[60] Law on Mass Media art. 1.

[61] Id. art. 2.

[62] Id. art. 3.

prohibited.[63] Journalists are responsible for verifying the trustworthiness of the information that they provide.[64]

Under the Mass Media Law, repeated violations of the Voting Rights and Referendum Law by a mass media outlet's editorial director will result in suspension of the outlet's activities.[65] The suspension must occur within five days of, but no later than the day before, election day, and if violations occur on election day, immediately.[66] Violations include conducting election campaigns contrary to Russian law. Dissemination in the course of an election campaign of materials or content for which the editorial director is not responsible is not considered a violation, however.[67]

IV. Other Government Actions

A. Open Registry of Fake News Sites

In order to further counter the spread of disinformation and fake news, the Russian government is planning to create an open registry of fake news with identification of the offending platforms and authors.[68]

B. International Cooperation

In 2018, the Russian Federation and Spain signed an agreement to join forces in countering fake news and cooperate in the area of cybersecurity. The agreement was signed after Spain accused Russian-based groups of trying to affect the outcome of a Catalan referendum for independence by spreading disinformation on social media platforms. Russian authorities vehemently denied these accusations but agreed to cooperate with Spain in setting up a joint cybersecurity group to prevent diplomatic relations from being damaged by the spread of disinformation.[69]

C. Review of the Activities of News Aggregators

According to media reports, the State Duma (the lower chamber of the Russian legislature) will discuss the activities of news aggregators with mass media representatives, a group of experts, and other parties, with the aim of minimizing the amount of disinformation distributed through

[63] Id. art. 4.

[64] Id. art. 49.

[65] Id. art. 16.1.

[66] Id.

[67] Id.

[68] *An Open Register of Fake News and Their Authors Will Appear in Russia*, RBC (May 15, 2019) (in Russian), https://perma.cc/P7LT-YRAN.

[69] *Russia and Spain Agree to Cooperate on Cyber Security, Fight Fake News*, Moscow Times (Nov. 7, 2018), https://perma.cc/DL9A-DKLT.

this medium.[70] The representatives are concerned by the fact that news aggregators sometimes keep banned content, including fake news.[71] In particular, the legislators stressed the importance of improving algorithms for the news ratings of the major Russian news aggregator, Yandex. According to representatives of Yandex, however, current legislation regulating mass media is sufficient, and mass media producers bear responsibility for their published content.[72]

V. Media Coordination

According to a report by Freedom House, foreign technology companies have not always complied with the demand of Roskomnadzor to remove questionable content.[73] Twitter complied with only 51% of 1,292 requests for content removal from July to December 2017. During the same period, Facebook restricted access to 174 items that violated "laws related to extremism, self-harm, suicide promotion, and unauthorized disclosure of personally identifiable information," and one item relating to defamation. Google received 12,060 requests from the Russian government to restrict content in that time frame and complied with 78% of the requests. Of those requests, 51% were based on national security grounds and 22% related to regulated goods and services.[74]According to the political ads placement policy of the major Russian social media network, VKontakte, while candidates can disseminate election propaganda, they cannot put ads of a political nature on their personal web pages or blogs or post announcements of political protests and other political activities. Under the Voting Rights and Referendum Law, campaign materials cannot be posted "outside the special Site section as determined by the social network administration."[75]

Placement of campaign related information on her social network personal page by a candidate for a district council seat in St. Petersburg became the subject of a judicial dispute in August 2019. A federal district court ordered removal of the candidate's name from the ballot and banned her from participating in the forthcoming municipal elections because her electoral opponent had accused her of using the largest Russian social network, VKontakte, for election purposes.[76] The court sided with the plaintiff, who saw illegality in the candidate's posting a note on her VKontakte site stating that she was registered as a candidate by the election commission and placing a hashtag calling for people to vote for her. The plaintiff asserted that the post constituted campaign advertising and, therefore, should be paid for from the candidate's official campaign fund, as with all other election materials.

---

[70] *The Duma in the Fall Will Return to Discuss the Work of News Aggregators*, Izvestiia (Aug. 19, 2018) (in Russian), https://perma.cc/X2GD-MUMN.

[71] Id.

[72] Id.

[73] *Russia, Key Developments: June 1, 2017 - May 31, 2018*, Freedom House, https://perma.cc/APZ3-MRY9.

[74] Id.

[75] VKontakte social network user agreement, https://perma.cc/7YSK-7M99.

[76] Krasnogvardeijskii District Court, St. Petersburg, case No. 2a-4990/2019, Aug. 22, 2019, https://perma.cc/ERT2-ZYYQ.

The court ruled that the social network is a computer program subject to copyright protection. It confirmed that the network can be used only for purposes established by the licensing agreement between the network and users. The court held that, because the agreement does not allow the posting of campaign materials on the personal sites of network users, the defendant conducted illegal campaigning, violated the licensing agreement, and breached the network's copyright. The court rejected the argument by the defendant's lawyer that the VKontakte rule addresses commercial advertisements only and does not relate to personal pages of network users where people inform others about themselves. The court also rejected the defense's argument that because the VKontakte system does not allow users to push information from their personal pages throughout the network, a personal posting cannot be considered a full-fledged advertisement and, therefore, the defendant's social media posting was not an act of campaigning.[77]

The adoption of anti-fake-news laws and laws prohibiting online publications containing disrespectful and insulting messages about the symbols of the Russian Federation, the Constitution, and the authorities has had a critical reception from the Russian media. Writers and journalists expressed the opinion that the newly passed laws restrict constitutional freedom of speech and "establish the right of an official, at his own discretion, without investigation and trial, by his sole decision, to forbid the dissemination of any information" and to indefinitely and "immediately" block any media resources on the internet.[84]

[77] *Russia: Court Removes Candidate from Ballot for Social Network Post*, Global Legal Monitor (Sept. 13, 2019), https://perma.cc/BPQ4-38HY.

[84] *Council of Federation Approves Anti-Fake-News Law and Law Prohibiting Disrespectful Treatment of Authorities*, NEWSru.com (Mar. 13, 2019) (in Russian), https://perma.cc/6CY6-Q24Q.

Sweden

Elin Hofverberg
Foreign Law Specialist

SUMMARY Sweden recognizes the right to free speech, including on the internet and through the use of social media platforms. While private entities are free to block inappropriate content, the government does not prohibit the use of Twitter or fake accounts on Twitter, and has not adopted legislation that allows for the blocking of internet sites or internet access by the government. It also does not regulate opinion-based advertisements. Sweden has, however, criminalized the dissemination of false information and requires news media to correct such information.

Recognizing that misinformation is a significant challenge globally, the Swedish government is in the process of launching a new agency, the Psychological Defense Agency, which will focus on psychological defense and combatting misinformation in Sweden. It is set to be launched in 2022. the Swedish Civil Contingencies Agency was earlier tasked with making Swedish residents aware of misinformation campaigns and educating them on how to verify the accuracy of information, and has been actively engaged in that process.

Media companies have begun to voluntarily address the misinformation problem. During the 2018 national election cycle, four Swedish public media corporations created a fact-checking website (now discontinued) that allowed members of the public to verify election-related claims. Bots were used in the 2018 election, but no successful misinformation campaigns were identified. Facebook deleted posts that included false information produced by fake accounts in connection with the national election in 2018. TV4 initiated rules prohibiting the purchase of political advertisements by foreign entities in the weeks leading up to 2019 EU parliamentary elections.

I. Background

A. Mass Dissemination of Information via Social Media

Misinformation continues to be one of the challenges facing Sweden from both a defense and civil contingencies perspective.[1] Mass dissemination is recognized by Swedish authorities as a global problem.[2] The risk of future mass dissemination of information in Sweden, especially as it relates to elections, is also recognized.[3] Fake Twitter accounts and automated accounts disseminated information over Twitter during the 2018 national election period, and the use of such methods

[1] MSB (Swedish Civil Contingencies Agency), *Five Challenging Future Scenarios for Societal Security*, 40, 54 (2013), https://perma.cc/QMT2-THDN.

[2] Id.; see also Nationell strategi för samhällets informations- och cybersäkerhet, Skr. 2016/17:213, https://perma.cc/3UAA-BQRY.

[3] Skr. 2016/17:213, *supra* note 2.

increased in the latter stages of the election period.[4] However, these disinformation attempts do not appear to have been successful.[5] Similarly, no successful disinformation campaigns were identified during the 2019 European Parliament elections. According to reports, ever since 2016, the internet has been used more than TV and newspapers combined to influence Swedish politics.[6] Swedish journalists also use social media as a source for their articles, which has resulted in some false reports, including a 2012 report of the death of British "Labour leader" Margaret Thatcher, the leader of the Conservative Party who was alive at the time.[7]

The Swedish Defense Research Agency (Totalförsvarets forskningsinstitut, FOI) has summed up the risks associated with foreign propaganda as follows: "Previously democracies risked becoming victims of an occupying power. Today, a foreign power may instead attempt to manipulate Swedish political elections through various kinds of information operations."[8]

B. Principles of Free Speech

Sweden protects the right to freedom of speech enshrined in its Constitution (Instrument of Government).[9] Further regulation of freedom of speech is done in two separate constitutional acts, the Freedom of the Press Act (Tryckfrihetsförordning, TF) and the Fundamental Law on Freedom of Expression (Yttrandefrihetsgrundlagen, YGL).[10] In addition, freedom of speech is protected in the European Convention on Human Rights,[11] to which Sweden is a party.

Sweden introduced its first freedom-of-the-press legislation in 1766.[12] The document was adopted by Royal acclamation, and removed the need for publishers to attain pre-approval from the King prior to publication.[13] A special fundamental law on freedom of expression covering nonprint

[4] Johan Fernquist et al., FOI, *Bots and the Swedish Election – A Study of Automated Accounts on Twitter* (Sept. 12, 2018), https://perma.cc/75PD-HZXM.

[5] Id.

[6] Nic Newman et al., Reuters Institute for the Study of Journalism, *Reuters Institute Digital News Report 2019*, https://perma.cc/8S7R-4DFB.

[7] Pär Anders Albinsson et al., FOI, *Analys och detection av vilseledning och paverkansoperationer i sociala medier* 13 (Dec. 2015), https://perma.cc/T2B2-EZMP.

[8] Niklas H. Rossbach, FOI, *Psychological Defence: Vital for Sweden's Defence Capability* 2 (Nov. 2017), https://perma.cc/9Y2H-ETLZ.

[9] Regeringsformen [RF] (Svensk författningssamling (SFS) 1974:152), https://perma.cc/2L66-LWKR.

[10] Tryckfrihetsförordning [TF] (SFS 1949:105), https://perma.cc/63C5-89AU; Yttrandefrihetsgrundlagen [YGL] (SFS 1991:1469), https://perma.cc/GB6Q-DLKC.

[11] European Convention on Human Rights [ECHR], Nov. 4, 1950, 213 U.N.T.S. 221, https://perma.cc/Y584-N9KT.

[12] Kongl. Maj:ts Nådige Förordning, Angående Skrif- och Tryck-friheten. Gifwen Stockholm i Råd-Cammaren then 2. December 1766, https://perma.cc/9BJA-9T6M.

[13] Id. 1 §. For more information on the 1766 law see Elin Hofverberg, *250 Years of Press Freedom in Sweden*, In Custodia Legis (Dec. 19, 2016), https://perma.cc/4NTL-78AR.

media was adopted in 1991.[14] Today the TF allows the legislature to put limits on freedom of the press, including through laws that limit the use of commercial advertisements, and criminalizes child pornography.[15]

Publishers of information on electronic databases are constitutionally protected,[16] but are also responsible for the content that appears on those databases.[17] Publishers of electronic bulletin boards (*elektroniska anslagstavlor*) are not responsible for the crimes that are committed using their services, such as comments posted by others, as the person posting the information is responsible for it.[18] Facebook has removed content that falsely proclaimed to be a Swedish Party Leader's account.[19]

II. Current and Pending Legislation

A. Treatment of Bots

The use of internet robots (bots) to automate the dissemination of information is not criminalized in Sweden. FOI produced a study on the use of Twitter bots in connection with the 2018 Swedish election,[20] which found that their use was widespread, but appeared less successful as the information was not retweeted by real accounts.[21]

B. Criminal Sanctions for Dissemination of Certain Information

Sweden has criminalized a number of acts that are related to the dissemination of propaganda. Those laws do not specifically mention dissemination via the internet or mobile apps, but also do not exempt these information channels.[22] For example, it is a crime (*högmålsbrott*, a type of treason) "to intentionally affect public opinion or limit the freedom of a political organization or a union or trade association to act and thereby jeopardize the freedom of speech and association" through the use of force, coercion, or criminal threats.[23] Accepting remuneration from foreign sources to

[14] For legislative background see Proposition [Prop.] 1990/91:64 om yttrandefrihetsgrundlag m.m., https://perma.cc/X878-7W3X.

[15] 1 kap. 12-14 §§ TF.

[16] 1 kap. 9 § 1 st YGL.

[17] Högsta Domstolen NJA 2013 s. 945, https://perma.cc/EHV3-LY72.

[18] NJA 2007 s. 805, https://perma.cc/65YS-DL3F.

[19] Antonia Woodford, *The Hunt for False News: EU Edition*, Facebook Newsroom (Apr. 2, 2019), https://perma.cc/7JVA-8PY8.

[20] Fernquist et al., supra note 4.

[21] Id.

[22] E.g., 18 kap. 5 Brottsbalken [BrB] (SFS 1962:700), e contrario, https://perma.cc/DLC6-E8A5.

[23] 18 kap. 5 § BrB.

spread propaganda in Sweden is also a crime,[24] as is spreading information that could be dangerous to the national security of Sweden.[25]

Information disseminated pertaining to the Swedish military is considered spying even if the information is false.[26] Thus, publishing fake news about Swedish military operations, military holdings, etc. is a crime.[27] Also, publishing certain documents that are deemed secret is criminalized, if publication risks the nation's security.[28] The accuracy of the information is not relevant. Any publication of such information, true or false, is a crime.[29] Other crimes include instigation of war (*krigsanstiftan*)[30] and upheaval (*uppror*),[31] crimes against a citizen's freedoms (*medborgerlig frihet*),[32] treason (*högförräderi*),[33] and threats against servants of the state (*hot mot tjänsteman*).[34] During times of war false rumors about the state are specifically criminalized.[35] Thus, Swedish media corporations may not publish information that risks the security of the state. It is the publisher (*ansvarig utgivare*) that is responsible for any violation.[36] In addition unlawful depictions of violence (*olaga våldsskildring*) are a crime.[37]

C. No Legal Authorization for Blocking Media

While the publication of certain information and statements (such as defamation, agitation of racial groups, and instigation of war) is criminalized, as can be seen from Part II(B), above, no legislation exists that allows the state to block media content because it is a threat to national security. Sweden has historically taken a stance against blocking or limiting internet access, arguing that "crimes should be prosecuted, not hidden."[38] It does however, allow "private individuals, schools, companies, or other organizations" to use filters to prevent access to "inappropriate material" (such as pornographic material) online. [39] Sweden is a member of the

[24] 19 kap. 13 § BrB.

[25] 7 kap 19 TF.

[26] Id.

[27] Id. 7 kap. 19 §.

[28] Id. 7 kap. 15 §.

[29] Id.

[30] 7 kap. 13 § TF.

[31] Id. 7 kap. 10 §.

[32] Id. 7 kap. 11 §.

[33] Id. 7 kap. 12 §.

[34] Id. 7 kap. 8 §.

[35] Id. 7 kap. 19 §.

[36] Id. 8 kap. 1 §.

[37] Id. 7 kap. 7 §.

[38] Konstitutionsutskottets betänkande2013/14:KU23Tryck- och yttrandefrihetsfrågor, at 26, https://perma.cc/CL6F-3KEZ.

[39] Id.

Freedom Online coalition, which encourages member states to work with private companies to prevent human rights violations online, and ensuring a free internet.[40]

D. Amended Advertisement Legislation

Swedish legislation on advertisements (the Advertisement Act)[41] does not include regulation of political, religious, or opinion-based advertisements. The government is currently working on amending the legislation, but the report published in connection with this does not address political advertisements.[42]

III. Other Government Actions

A. Creation of Psychological Defense Authority

In 2018 the Swedish government announced that it would launch a new Psychological Defense Authority,[43] because creating such an authority was an "important step in the process of building a modern total defense adapted to the threats of our time."[44] The purpose of the authority is to

> discover, counter, and prevent influence campaigns, and disinformation, both nationally and internationally. It shall also strengthen the population's resistance [so that people can] themselves discover influence campaigns and disinformation. In addition, the psychological defense must be able to act both in the short term and in the long term. [45]

The mission of the Psychological Defense Authority will be to "identify, analyze, and counter influence campaigns."[46] Originally, the commission for the creation of the Psychological Defense Authority was scheduled to present a report on how this authority could be created no later than August 15, 2019.[47] On July 11, 2019, this date was extended to May 31, 2020.[48] The government hopes the institution will be in place by 2022 (which is also the next election year).[49]

---

[40] *About us*, Freedom Online Coalition, https://perma.cc/8R8W-SUUN

[41] Marknadsföringslag [Advertisement Act] (SFS 2008:486), https://perma.cc/SSG6-244P.

[42] Statens Offentliga Utredningar [SOU] 2018:1 Ett reklamlandskap i förändring – konsumentskydd och tillsyn i en digitaliserad värld, https://perma.cc/9UWJ-WZKB.

[43] DIR 2018:80 Ansvar, ledning och samordning inom civilt försvar, https://perma.cc/GCF8-Z6HV.

[44] DIR 2018:80, at 7 (translation by author).

[45] DIR 2018:80, at 5.

[46] DIR 2018:80, at 7 (translation by author).

[47] DIR 2018:80, at 10.

[48] Tilläggsdirektiv till Utredning om en ny myndighet for psykologiskt försvar (Ju 2018:06) Dir. 2019:42, https://perma.cc/5P4P-SM5W.

[49] Press Release, Länsstyrelsen för Västra Götaland, Landshövdingen ska utreda ny myndighet (June 3, 2019), https://perma.cc/HRZ5-8NX6.

According to FOI, counteracting deception, disinformation ("including rumour-mongering"), and propaganda is one of three essential components of psychological defense.[50] Psychological defense is thus, according to FOI, about creating a psychological climate—"a will to defend" and "a coordinated narrative about what values Sweden wishes to uphold."[51]

B. Nordic Cooperation on Cyberattacks and Foreign Influence

In a 2017 op-ed, the Danish and Swedish Ministers of Defense declared that "fake news" is a danger to the two countries.[52] The Nordic countries have collectively joined forces to combat fake news, proposing coordination of their national security strategies.[53]

C. Civil Contingency Agency Tasked with Increasing Misinformation Literacy of Citizens

In addition to the above measures, Sweden has worked to increase the misinformation literacy of its citizens. The Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB) was specifically tasked with increasing the awareness among Swedish residents of the threats associated with misinformation and influence campaigns.[54] One of the MSB's responses was the publication in 2018 of *Countering Information Influence Activities: A Handbook for Communicators*,[55] which provides communicators working in public administration with resources in the event of an actual or anticipated information influence campaign.

As early as 2013 the MSB recognized that misinformation was one of the possible crisis scenarios that Sweden would have to address in the future.[56] The MSB response includes a public emergency preparedness brochure on how to act "when crisis or war comes."[57] This publication includes information on how to spot fake news and misinformation campaigns.[58]

---

[50] Rossbach, supra note 8, at 1-2. "The three parts are: to counteract deception and disinformation, including rumour-mongering and propaganda or, in other words, everything that hostile psychological warfare engages in; to ensure that the government authorities can get their message out in a crisis, including war; and to contribute to strengthening the population's will to defend Sweden." Id.

[51] Id. at 3.

[52] Peter Hultqvist & Claus Hjort Frederiksen, *Ryska 'fake news' - en fara för våra länder*, Aftonbladet (Aug. 30, 2017), https://perma.cc/5QF2-ZMXS.

[53] Press Release, Nordic Council, Nordic Fightback against Fake News (Oct. 30, 2018), https://perma.cc/W8YL-LABR.

[54] MSB regleringsbrev, Regleringsbrev för budgetåret 2019 avseende Myndigheten för samhällsskydd och beredskap, ESV (Dec. 20, 2018), https://perma.cc/H94V-RXV7.

[55] MSB, *Countering Information Influence Activities: A Handbook for Communicators* (Mar. 2019), https://perma.cc/3L7W-YJ2Y.

[56] MSB, *Five Challenging Future Scenarios for Societal Security* (Mar. 2013), https://perma.cc/7CB5-DTKR.

[57] MSB, *Om Krisen eller Kriget Kommer* (May 2018), https://perma.cc/4PHH-ZCQG.

[58] Id. at 6.

IV. Media Coordination

A. Industry Fact-Checking Sites

During the 2018 parliamentary election cycle a joint initiative to address fake news titled *Faktiskt.se* ("actually") was created.[59] Faktiskt.se was a collaboration between the two largest morning newspapers, Dagens Nyheter (DN) and Svenska Dagbladet (SVD), and the two public service providers, Sveriges Radio (SR) and Sveriges Television (SVT).[60] It evaluated the accuracy of political statements by political party leaders,[61] as well as other news stories—for example, on the reported health benefits of moderate alcohol use.[62] It was discontinued in December of 2018 following the election, as originally planned.[63]

TV Broadcaster TV4 (owned by Bonnier) has published rules on who may advertise, and specifically who may purchase political advertisements to be broadcast in Sweden.[64] During the most recent election to the European Parliament (three weeks prior to the May 26, 2019, vote) only Swedish political parties and Swedish unions were allowed to advertise political messages.[65]

B. Self-Regulation of Journalistic Content

Swedish journalists are bound by industry ethical guidelines (Ethical Rules for Press, TV, and Radio) and have a general duty to correct information that is false.[66] Swedish journalists are typically not prosecuted for misinformation, but are criticized by the Press Council (PON) following referral from the Press Ombudsman (PO).[67] The PO is responsible for investigating, at the request of an individual or on its own initiative, possible violations of "the use of good publishing practices," which include accuracy of the information published.[68] The PO refers cases to the PON when it finds that a violation has taken place.[69] The PO's review specifically includes social media content.[70] The PON has previously explained that "[a] fundamental prerequisite for publishing must be that publishing is compatible with good publishing customs and that there is

[59] Faktiskt.se, https://perma.cc/QCF8-6NC6/.

[60] Id.

[61] Faktakollen, SVT, https://perma.cc/VU99-4S6F; *Ebba Busch Thor har delvis rätt om vårdköer*, SVT (Oct. 31, 2018), https://perma.cc/3ERY-KK6V.

[62] Faktakollen, SVT, https://www.svt.se/nyheter/inrikes/17565278; *Därför är påståendet om att alkohol kan vara nyttigt mestadels fel*, SVT (Nov. 3, 2018), https://perma.cc/9XZ2-V378.

[63] Linnéa Kihlström, *Faktiskt.se läggs ned*, Medievärlden (Oct. 11, 2018), https://perma.cc/6RV7-HA8A.

[64] *Regler för åsiktsannonsering i TV4*, Bonnier Broadcasting (Mar. 29, 2018), https://perma.cc/B5BU-LUB6.

[65] Id. § 7.

[66] *Etiska regler for press, TV och radio*, PO-PON, https://perma.cc/94CB-AS7L.

[67] *Senaste fällningar*, PO-PON, https://perma.cc/ME5M-FQ8U.

[68] PO-PON, 1 § Instruktion for Allmänhetens Pressombudsman, https://perma.cc/S2C7-GZL4.

[69] Id.

[70] Id. 1 § c.

evidence to substantiate the information."[71] Thus, the publication of false information violates the ethical rules. The maximum fine to be paid by the publisher for such violations is SEK 32,000 (about US$3,500).[72]

[71] *Svenska Dagbladet klandras för publicering om NN [namn angivet]*, PO-PON (June 25, 2018), https://perma.cc/VKR6-C8EA; *see also* Elin Hofverberg, *Sweden: Swedish Media Criticized by Swedish Press Council for Publishing Names of #MeToo Accused Without Cause*, Global Legal Monitor (Oct. 4, 2018), https://perma.cc/Y3BQ-K6KM.

[72] *Hur går det till?*, PO-PON, https://perma.cc/7BCD-QYKE.

United Arab Emirates

George Sadek
Foreign Law Specialist

SUMMARY There are three legislative instruments governing the issue of transparency and spreading of misinformation on social media: Federal Law No. 5 of 2012, Federal Law No. 12 of 2016, and the Electronic Media Regulation of 2018. A number of individuals have been brought before the courts of the United Arab Emirates for violating provisions of Federal Law No. 5 of 2012.

In addition to issuing legislative tools and referring violators to court, the Emeriti authorities have adopted a number of measures to combat the phenomenon of posting false information online or through social media. These measures include the blocking of misinformation, a public awareness campaign, and the creation of a course curriculum for the purpose of educating students about false news in the digital age.

The government of the Emirate of Dubai publicized a June 2019 dialogue between local journalists and Facebook addressing false news on social media.

I. Background

The Dubai Police Force has blocked 5,000 fake social media accounts since 2017, in cooperation with the Telecommunication and Regulatory Authority (TRA).[1]

To combat misinformation circulating on social media, the police force announced that it has conducted a public awareness campaign across various social media platforms, with educational clips and posters to educate the public on how to identify and report fake accounts on social media.[2]

In March 2018, the National Media Council issued new regulations governing all online activities, including e-commerce; the publishing and selling of print, video, and audio material; and advertising. Under the regulations, social media influencers and advertisers who engage in commercial transactions must apply for licenses to operate.[3]

[1] Ali Al Shouk, *Faking Social Media Accounts Could Land You in Jail*, Gulf News (Feb. 10, 2019), https://perma.cc/U62Q-PGM4.

[2] Id.

[3] *Freedom on the Net 2018: United Arab Emirates*, Freedom House (undated), https://perma.cc/XAB2-MUVX.

II. Current Legislation

There are three legislative instruments governing transparency and misinformation on social media: Federal Law No. 5 of 2012,[4] Federal Law No. 12 of 2016,[5] and the Electronic Media Regulation of 2018.[6]

A. Federal Law No. 5 of 2012

Federal Law No. 5 of 2012, issued on August 13, 2012, is aimed at combating a number of offenses, including sharing and posting online content that violates the privacy of others, insulting the symbols of the state and religions, calling for overthrowing the government of the UAE, and disseminating hate speech and inciting violence.

Article 21 of the Law punishes whoever uses a computer network, electronic information system, or any tools of information technology to invade the privacy of another person with a term of imprisonment of at least six months and a fine between 150,000 UAE dirhams (around US $40,830) and 500,000 UAE dirhams (around US $136,102) or either of these two penalties. Article 21 paragraph 2 enhances the penalty to a period of imprisonment of at least one year and a fine between 250,000 UAE dirhams (around US $68,000) and 500,000 UAE dirhams (around US $136,102) or either of these two penalties when a person uses an electronic information system or any information technology means to alter a record, photo, or scene for the purpose of insulting, offending, attacking, or invading another person's privacy.[7]

Article 24 stipulates that whoever establishes, administers, and runs a website or publishes on a computer network or any method of information technology online content promoting rioting, hatred, racism, sectarianism, or damage to the national unity or social peace or disturbance of the public order and public morals must be punished by imprisonment and a fine between 500,000 UAE dirhams (around US $136,102) and one million UAE dirhams (around US $272,204).[8]

Article 28 provides that whoever establishes, manages, or runs a website or uses information on a computer network or any means of information technology to transmit information, news, or cartoon drawings or any other pictures for the purpose of endangering the national security and the higher interests of the State or to disturb the public order must be punished by a period of imprisonment and a fine not to exceed one million UAE dirhams (around US$272,204).[9]

Under article 29, whoever publishes information, news, statements, or rumors on a website or any computer network or by any means of information technology to damage the reputation, prestige, or stature of the State or any of its institutions or its president, vice-president, any of the

[4] Federal Law No. 5 of 2012, Al-Jaridah Al-Rasmiyah, vol. 540 (13 Aug. 2012), https://perma.cc/R62R-UMZC.

[5] Federal Law No. 12 of 2016, Al-Jaridah Al-Rasmiyah, vol. 597 (31 May 2016), https://perma.cc/B38N-VDNF.

[6] National Media Council, *Electronic Media Regulation* (undated), https://perma.cc/6EM8-3MV8.

[7] Federal Law No. 5 of 2012, art. 21.

[8] Id. art. 24.

[9] Id. art. 28.

rulers of the Emirates, their crown princes, the State's flag, the national peace, the Emirates' coat of arms, the national anthem or any of the national symbols must be punished by imprisonment and a fine not exceeding one million UAE dirhams (around US$272,204).[10]

Under article 30, whoever establishes, manages, or runs a website, or publishes information on a computer network or by means of information technology to overthrow the State, change or seize its ruling system, or violate the country's constitution or laws or oppose the basic principles that constitute the foundations of the State's ruling system must be punished by life imprisonment.[11]

Likewise, article 38 stipulates that whoever publishes online any incorrect, inaccurate, or misleading information that damages the interests of the State or tarnishes its reputation, prestige, or stature must be punished with a term of imprisonment.[12]

Finally, under article 39, any person who fails to remove or block access to illicit content after receiving a notice from the federal authorities faces a term of imprisonment, a fine, or both.[13]

B. Federal Law No. 12 of 2016

Federal Law No. 12 of 2016 amends article 9 of Federal Law No. 5 of 2012 by enhancing the penalty for creating an account using a fake internet protocol (IP) address. It states that whoever uses a fraudulent IP address by using a false mailing address or a third-party address or by any other means for the purpose of committing a crime or preventing its discovery will be punished by a term of imprisonment and fine between 500,000 UAE dirhams (around US$136,102) and two million UAE dirhams (around US$544,408).[14]

C. Electronic Media Regulation of 2018

The Electronic Media Regulation of 2018 defines electronic media as an activity carried out through electronic methods to publish and disseminate information. It aims at regulating information on social media to provide a responsible content that does not violate the privacy of individuals and protects society.[15]

[10] Id. art. 29.

[11] Id. art. 30.

[12] Id. art. 38.

[13] Id. art. 39.

[14] Federal Law No. 12 of 2016, art. 9.

[15] National Media Council, *supra* note 6, at 2.

The regulation requires the following acts to be licensed by the National Media Council:

> 1- Online trade, present and sell print, video, and audio materials.
> 2- The electronic publishing activities and on call printing.
> 3- The specialized websites such as the electronic advertisements, news sites, etc.) [sic].
> 4- Any electronic activity that the council deems appropriate to be added.[16]

The regulation obliges individuals carrying out media activities using social media to obtain a license from the national media council. The following requirements must be met:

> 1-There should be a recognized social media account.
> 2-The advertisements circulated on the social media shall meet the applicable advertising standards or criteria adopted by the council.
> 3-The social media account holders providing paid commercials shall obtain a license from the National Media Council in accordance with the applicable regulations and those prescribed in this regulation.
> 5- The account holder shall be responsible for the content of such account.[17]

The National Media Council was created by Law No. 11 of 2016.[18] It is composed of a Chairman[19] and a Board of Directors selected by the Cabinet.[20] The Council is responsible for drafting the media policies of the state and formulating media legislation.[21] Furthermore, it provides the licensing and permission for media activities, including electronic and print media.[22]

III. Court Cases

A number of individuals have been charged with violating provisions of Federal Law No. 5 of 2012, and some have been convicted by the courts of the United Arab Emirates.

A. Jodi Magi Case

In July 2015, an Abu Dhabi court found Jodi Magi, a Zayed University employee, guilty of posting inappropriate content on her Facebook account. The Australian woman was convicted and taken into custody pending her deportation.[23]

---

[16] Id.

[17] Id. at 5.

[18] Federal Law No. 11 of 2016, Al-Jaridah Al-Rasmiyah, vol. 597 bis, 23 May 2016.

[19] Id. art. 8.

[20] Id. art. 6.

[21] Id. art. 4.

[22] Id. art. 5(4).

[23] Neil Halligan, *Australian Woman Jailed in Abu Dhabi over Facebook Post*, Arabian Bus. (July 14, 2015), https://perma.cc/TF3T-C5CY.

Magi had posted a picture of a car parked across two disabled parking spaces outside her apartment.[24] Before her trial, Magi reportedly attempted to pay a fine of 10,000 UAE dirhams (around US$2,722) and leave the country of her own accord but the Emirati authorities insisted that she stand trial.[25]

B. Mansour Al Shahi Case

Ahmed Mansour Al Shahi was accused of using social media, particularly Twitter and Facebook, to publish fabricated news in violation of Federal Law No. 5 of 2012.[26] There is no information available about what, exactly, Al Shahi allegedly posted on social media.

The Abu Dhabi Union Appeal Court found Al Shahi guilty in May 2018 of spreading false stories and information that harmed the country's reputation and its foreign policies. It sentenced him to ten years' imprisonment and a fine of one million UAE dirhams (about US$272,201). The Union Supreme Court rejected Al Shahi's appeal.[27]

C. Claimed Abduction Case

In October 2018, the Abu Dhabi Police Force detained two women who posted a video on social media of a woman of African origin carrying an Emerati child on a street in Abu Dhabi's Al Shamkha district. The two women posters allegedly claimed it was an incident of child abduction. The police determined that the woman recorded on the video was the child's nanny, who was taking the child for a walk at the mother's instruction.[28]

The posters are charged with disseminating false information on social media. The case has been referred for prosecution to the Abu Dhabi Judicial Department.[29]

IV. Other Government Actions

In addition to issuing legislative tools and referring violators to court, the Emeriti authorities have adopted a number of measures to combat the phenomenon of posting false information online or through social media. Those measures include the blocking of misinformation, a public awareness campaign, and the creation of a course curriculum for the purpose of educating students about false news in the digital age.

---

[24] Id.

[25] Sophie McNeill, *Australian Woman Jailed in Abu Dhabi for "Bad Words" Posted on Social Media*, ABC Australia (July 13, 2015), https://perma.cc/E94U-JMYM.

[26] Mustafa Al Zarooni, *Emirati Fined Dh1 Million, Jailed for Publishing Fake News*, Khaleej Times (Jan. 1, 2019), https://perma.cc/6BZE-YQC7.

[27] Id.

[28] Mariam Al Serkal, *Two Sisters Held in Abu Dhabi for Posting Fake News,* Gulf News (Oct. 10, 2018), https://perma.cc/BQU5-HPUX.

[29] Id.

A. Blocking Misinformation

The Federal Telecommunication Regulatory Authority instructs internet service providers to block any online content promoting violence, pornography, and political speech. In 2017, the Authority blocked a number of Qatari media websites, including Al-Jazeera Live, Peninsula Qatar, the Arabic Huffington Post, and the Muslim Brotherhood official website.[30]

B. Public Awareness Campaigns

In October 2018, the Abu Dhabi Police Force launched a public awareness campaign to educate the public about Federal Law No. 5 of 2012 on cybercrimes and penalties imposed on violators. Additionally, the police organized a workshop to warn the public of the danger of false news that might circulate on social media. Speakers at the workshop stressed that teachers can play a key role in educating students on how to identify false information on social media.[31]

Similarly, following a period of flash flooding in 2019, the Emirate of Ras Al Khaimah Police posted a warning on Instagram to residents of Ras Al Khaimah not to disseminate any unverified information on social media related to the weather in the emirate.[32]

C. Course Curriculum

To educate youth about the danger of misinformation circulating on social media outlets, the International Baccalaureate schools in the UAE announced in April 2019 that they will introduce a course on best methods to deal with false news on social media. The course will also address the effect of social media on society.[33]

D. Identification of Foreign Influence Campaigns

In April 2018, the UAE's Minister for Foreign Affairs, Anwar Gargash, accused Iran of being the foreign source disseminating false news in both the UAE and Saudi Arabia. Gargash tweeted that Iran's Fars News Agency and a newspaper affiliated with the Hezbollah militia, Al Akhbar, constantly spread fake news about the UAE and the Kingdom of Saudi Arabia.[34]

---

[30] *Freedom on the Net 2018*, *supra* note 3.

[31] Amira Agraib, *Dh1 Million Fine for Spreading Rumours, Fake News in UAE*, Khaleej Times (Oct. 14, 2018), https://perma.cc/4S2R-TFEA.

[32] Aisha Victoria Deeb, *Dhs 1 Million Fine for "Fake News" about the Weather in the UAE*, Mashable Middle East (Apr. 15, 2019), https://perma.cc/WBR3-FZH4.

[33] Sarwat Nasir, *IB Schools in UAE to Teach Kids How to Spot "Fake News,"* Khaleej Times (Apr. 21, 2019), https://perma.cc/NZF2-N2DC.

[34] *UAE's Gargash Denies Reports of Tension with Saudi Arabia*, National (Apr. 18, 2018), https://perma.cc/3JRG-AAJS.

V. Media Coordination

The government of the Emirate of Dubai publicized on its media office web page a June 2019 dialogue between journalists and Facebook that was hosted by the Dubai Press Club.[35] Key issues discussed in the dialogue included journalistic integrity, how to combat the dissemination of false news on social media, and how the Facebook algorithm works.[36]

[35] *Facebook News Forum Discusses Future of News Industry*, Dubai Gov't Media Off., (June 19, 2019), https://perma.cc/PYE5-2GMD.

[36] Anupa Kurian-Murshed, *Facebook in Dubai Meet-Up Agrees that They Might be Slow to React Sometimes to Troll Farms*, Gulf News (June 19, 2019), https://perma.cc/WC8W-MR4F.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY "Fake news" has recently been recognized in the United Kingdom as an issue that poses a potential national security threat, with foreign actors seeking to influence UK citizens. The UK does not currently have any legislation that regulates the validity of news posted by online platforms, but proposed legislation is pending. Several government reports issued on this subject have recommended the introduction of a duty on tech companies to remove content identified as harmful or face fines. The government has also introduced a number of initiatives to counter misinformation by providing models for government departments to follow when distributing accurate information. In addition it has introduced a campaign called "Don't Feed the Beast" designed to increase awareness for residents in the UK when reading and distributing online information.

The UK does have legislation regulating political speech on traditional broadcast media, but this does not extend to political advertisements distributed digitally. The UK's system of regulating campaign financing focuses on limiting the expenditure of political parties, individual candidates, and third parties rather than limiting donations that can be received by these parties and individuals, combined with a transparent reporting system of donations received and election expenditure incurred. Donations above a certain amount must be reported. Political parties receive a certain amount of broadcasting time on national television and radio free of charge.

The government has introduced a number of initiatives to help counter misinformation distributed online. The Fusion Doctrine provides that the intelligence services are responsible for identifying social media platforms that distribute misinformation and disinformation. The Rapid Response Unit was established within the Cabinet Office to help ensure debates are fact-based. The National Security Communications Team's purpose is to tackle communications elements of threats to national security, including (but not limited to) disinformation. These initiatives are designed to enable the government to publish factual information in a timely fashion to counter any misinformation, along with the campaign to educate citizens on how to detect misinformation and disinformation.

Traditional broadcast media are subject to legislation requiring channels to ensure that any news is accurate and impartially provided. They are also subject to strict limitations over political broadcasts. The Office of Communications, which has the authority to impose financial penalties and revoke broadcasting licenses, is responsible for regulation in this area. Online media are currently not subject to the same restrictions as traditional broadcast media, but the government is considering introducing legislation to regulate this area.

I. Background

Misinformation is not a new phenomenon in the United Kingdom. In 1688, the Privy Council issued a proclamation that prohibited spreading false information.[1] Modern information technology like digital and social media platforms now facilitates the dissemination of false information to wide audiences.[2] The government has noted that,

> [i]n the era of fake news and concerted propaganda by hostile states, supporting a free media also means countering the incoming tides of disinformation. While it has never been easier to publish and receive information, it has also never been easier to spread lies and conspiracy theories. Social media offers a malign opportunity to whip up hatred and incite violence against vulnerable minorities.[3]

The government considers that misinformation and disinformation are "fourth generation espionage" and are taking action on multiple levels to help counter this threat.[4] It notes that a "whole-of-society approach to defensive and offensive measures in the information space is necessary to ensure protection against physical and cognitive attack and subversion of society, for example, through legislation and execution."[5] The Digital, Culture, Media and Sport (DCMS) Committee has recommended that the government not use the term "fake news" and instead use the words "misinformation" and "disinformation."[6] The government has defined these terms as follows:

> [D]isinformation [i]s the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain. 'Misinformation' refers to the inadvertent sharing of false information.[7]

The DCMS Committee released a report on fake news and misinformation in late February 2019. In this report, the committee's chair, Damian Collins, stated,

> [w]e need a radical shift in the balance of power between the platforms and the people. The age of inadequate self regulation must come to an end. The rights of the citizen need

[1] By the King, a Proclamation to Restrain the Spreading of False News (Oct. 26, 1688), https://perma.cc/T5YD-78EG.

[2] HM Government, *National Security Capability Review* 34 (2018), https://perma.cc/7FVT-3PFL.

[3] *Britain Champions Free Speech, So We're Leading the War on Fake News: Article by Jeremy Hunt*, gov.uk (Nov. 1, 2018), https://perma.cc/X7YW-MZNK.

[4] Speech by MI6 Chief Alex Younger, Fourth Generation Espionage (Dec. 3, 2018), https://perma.cc/9GUH-C2VC.

[5] Ministry of Defence, *Global Strategic Trends: The Future Starts Today* 16 (6th ed. 2018), https://perma.cc/S8HV-7WK3.

[6] House of Commons DCMS Committee, *Disinformation and 'Fake News': Interim Report*, HC 363 (2018) ¶ 14, https://perma.cc/DF8J-4PDG.

[7] House of Commons DCMS Committee, *Disinformation and 'Fake News': Government Response to the Committee's Fifth Report of Session 2017–19*, HC 1630 (2018) 2, https://perma.cc/E92S-4GGC.

> to be established in statute, by requiring the tech companies to adhere to a code of conduct written into law by Parliament, and overseen by an independent regulator.[8]

While the government is in the process of considering various options to stop online misinformation, the government has stated that, in the current moment, there are three challenges it faces when tackling the spread of misinformation:

- Identifying it
- Choosing how to respond to such information
- Ensuring that government information is available and "highly visible to the public" to reassure citizens of the facts, rather than working to rebut the false information[9]

Government strategy towards tackling "fake news" has two aspects: preemptive responses aimed to counter misinformation surrounding predictable events, such as elections, and responses that follow a predetermined plan for unforeseen events.[10]

While the government is seeing an increase in the spread of misinformation, the challenge of how to take action to mitigate this has to be balanced with the right of freedom of expression, as provided for by the European Convention on Human Rights and incorporated into the national law of the United Kingdom by the Human Rights Act 1998.[11] Article 10 of the European Convention on Human Rights provides for freedom of expression and grants individuals the right to hold opinions, and to receive and share ideas, without state interference. It specifically includes politics and matters of public interest:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.[12]

Under the Human Rights Act 1998, freedom of expression is a qualified right, which means that it may be restricted in certain circumstances provided it is prescribed by law and necessary in a democratic society to protect a legitimate aim. Article 10(2) specifies as follows:

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the

[8] Ofcom, *Addressing Harmful Online Content* 2 (Sept. 18, 2018), https://perma.cc/ZPN9-BWK7.

[9] Government Communication Service, *5 Trends in Leading-Edge Communications* 7 (Oct. 2018), https://perma.cc/4BDP-JTRN.

[10] Id.

[11] Human Rights Act 1998, c. 42, https://perma.cc/ZKN8-XVNC.

[12] Id. sched. 1, art. 10(1).

> disclosure of information received in confidence, and for maintaining the authority and impartiality of the judiciary.[13]

The UK government has noted that freedom of expression

> does not protect statements that unlawfully discriminate against or harass, or incite violence or hatred against, other persons and groups, particularly by reference to their race, religious belief, gender or sexual orientation . . . [and] [n]o one can rely on the human right to freedom of expression to limit or undermine the human rights of others.[14]

The European Court of Human Rights has determined that whether the restriction on freedom of expression is necessary "requires the existence of a pressing social need, and that the restrictions should be no more than is proportionate."[15] The UK's Equality and Human Rights Commission has stated that "[f]reedom of expression is protected more strongly in some contexts than others. In particular, a wide degree of tolerance is accorded to political speech and debate during election campaigns."[16] The European Court of Human Rights has similarly stated that "it is particularly important in the period preceding an election that opinion and information of all kinds are permitted to circulate freely."[17]

II. Current and Proposed Legislation

A. Current Legislation to Prevent Misinformation

The UK currently does not have legislation specifically designed to ensure the accuracy of news and information provided exclusively online. While there is currently no legislation that prohibits the online publication of misinformation or disinformation, the government is investigating the impact of such news and the possibility of introducing legislation:

> Traditional channels have been largely discarded in favour of digital and social media platforms. This is combined with a decline of trust in traditional sources of information and the era of so-called 'fake news'. In parallel, the rules of the game have changed. The democratization of information, and the means to exploit it, has allowed hostile actors to exert disproportionate influence in competition with the public interest.[18]

> If 'fake news' is tolerated and becomes commonplace, there would be grave consequences for public attitudes, democratic processes and for the conduct of public life. The risks increase with the growth in the use of social media, but the associated problems would not be confined to such material. Without reassurance that the false and the genuine are being distinguished, there is a real risk of "contamination" across all sources – with public trust

[13] Id. sched. 1, art. 10(2).

[14] Equality and Human Rights Commission, *Guidance: Legal Framework: Freedom of Expression* 5 (Mar. 2015), https://perma.cc/A8C9-HAJL.

[15] Ursula Smartt, *Media & Entertainment Law* 64 (3d ed. 2017).

[16] Equality and Human Rights Commission, supra note 14, at 4.

[17] Bowman v. United Kingdom (1998) 26 EHRR 1, https://perma.cc/6VTX-WU7P.

[18] HM Government, supra note 2, at 34.

> and confidence in public life declining further still, whatever the origin of the information or its channel of communication. As the problem gets worse, mere allegations will undermine the credibility of facts which actually are accurate.[19]

The UK does not have a regulatory body that oversees the various social media platforms and online written content as a whole. The closest regulatory body to address these types of issues is the Office of Communications (Ofcom), established under the Communications Act 2003 to enforce content standards across television and radio broadcasters, including rules that require accuracy and impartiality, and this is discussed further below.[20] Ofcom has argued the regulation of television and radio broadcasting and lack of regulation of online content has led to "a 'standards lottery' that allows social media platforms to take advantage of lax regulation while traditional broadcasters have to follow tough rules on protecting audiences."[21]

The Information Commissioner is also currently[22] "investigating the use of personal data and analytics by political campaigns, parties, social media companies and other commercial organisations."[23]

B. Proposals to Regulate Misinformation

1. Recommendations in the Cairncross Review

A number of government reports[24] have recently been issued that, among other issues, consider whether the UK should introduce laws to regulate the accuracy of news on online platforms. In 2019 the government published a report known as the *Cairncross Review* that determined, among other things, that "[i]nvestigative journalism and democracy reporting are the areas of journalism most worthy and most under threat [and] . . . that, given the evidence of a market failure in the supply of public-interest news, public intervention may be the only remedy."[25] The *Cairncross Review* recommended that every online platform should have a quality obligation for any news

[19] Richard Thomas, *Fake News and the Nolan Principles*, Committee on Standards in Public Life (Mar. 6, 2017), https://perma.cc/KQM7-JMFF.

[20] Communications Act 2003, c. 21, https://perma.cc/5NAX-VJH7.

[21] Aliya Ram & Nic Fildes, *Ofcom Outlines Case for Regulating Social Media Networks*, Financial Times (London) (Sept. 18, 2018) (by subscription).

[22] *Investigation into Data Analytics for Political Purposes*, Information Commissioner's Office (undated), https://perma.cc/Y69T-DDXQ.

[23] *The Rise of Digital Campaigning*, The Electoral Commission (undated), https://perma.cc/RZ54-S6FG.

[24] See, e.g., Cabinet Office, *Protecting the Debate: Intimidation, Influence and Information* (July 2018), https://perma.cc/BC2B-B2YQ; The Cairncross Review, *A Sustainable Future for Journalism* 7 (Feb. 2019), https://perma.cc/624J-37RW; HM Government, *Online Harms White Paper* CP 57 (2019), https://perma.cc/6D3L-X72F.

[25] The Cairncross Review, supra note 24, at 7.

on its platform and that the platform should be overseen by a regulator with investigative powers.[26] The review made several other key recommendations, including the following:

- Placing online platforms under regulatory supervision
- Introducing "codes of conduct to rebalance the relationship between publishers and online platforms"[27]
- Creating a new, independent, Institute to help continue the future provision of public-interest, regional, and local news[28]
- Introducing tax relief to encourage the payment for online news content
- Developing a media literacy strategy[29]

2. White Paper Recommendations

The government recently published a white paper, entitled *Online Harms*, which proposes a new regulatory framework that would clarify the responsibilities of companies to keep online users in the UK safer online and includes action that can be taken to counter illegal content and activity.[30] With regard to Facebook, the white paper noted that

> Facebook's handling of personal data, and its use for political campaigns, are prime and legitimate areas for inspection by regulators, and it should not be able to evade all editorial responsibility for the content shared by its users across its platforms.[31]

The white paper aims to establish a framework "ensuring disinformation is tackled effectively, while respecting freedom of expression and promoting innovation."[32] It recommends that laws be introduced to establish a legal duty of care for companies that host online content and to require tech companies to act to remove harmful or illegal content hosted on their platforms or sites.[33] Compliance with this duty of care would be overseen by a newly created independent regulator, which would have statutory powers to commence legal action against tech companies that breach this duty, along with the ability to impose substantial fines.

---

[26] Press Release, Department for Digital, Culture, Media & Sport and The Rt Hon Jeremy Wright MP, Cairncross Report Recommends Levelling of the Playing Field for UK Journalism (Feb. 12, 2019), https://perma.cc/WNK8-659G.

[27] The Cairncross Review, supra note 24, at 10.

[28] Id.

[29] Id.; Press Release, supra note 26.

[30] HM Government, *Online Harms White Paper*, supra note 24.

[31] House of Commons DCMS Committee, *Disinformation and 'Fake News': Final Report*, 2019, HC 1791, https://perma.cc/5H2X-G2WU.

[32] Home Office in the Media Blog: Monday 18 February (Feb. 18, 2019), https://perma.cc/3BJ4-QK8S.

[33] *Democracy Is at Risk from the Relentless Targeting of Citizens with Disinformation*, House of Commons (Feb. 18, 2019), https://perma.cc/LM8H-R2XV.

The committee recommended that any new regulator be funded through a levy on tech companies operating in the UK.[34] The committee further recommended that a new category be created for social media companies to tighten the liabilities of tech companies that are "not necessarily either a 'platform' or a 'publisher.' This approach would see the tech companies assume legal liability for content identified as harmful after it has been posted by users."[35]

The current regulator for traditional broadcast media, Ofcom, responded positively to the recommendation of placing responsibility on platforms for the content that they host.[36] Ofcom itself has called for more regulation over social media, specifically Facebook, YouTube, and Twitter, and has called for regulation that would require the platforms to quickly and effectively remove inappropriate content or be fined.[37] Ofcom has further proposed that transparency should be increased across all platforms to enable audiences to understand why they are being targeted by certain material.[38] Both Ofcom and the DCMS Committee have proposed that "the Government [should use] the rules given to Ofcom under the Communications Act to set and enforce contents standards for television and radio broadcasters, including rules relating to accuracy and impartiality, as a basis for setting standards for online content."[39]

C. Current Legislation Regulating Online Political Advertisements

A report from the House of Commons DCMS Committee has noted a significant increase in political parties' spending on Facebook advertisements in the past two general elections. In 2015, spending was around £1.3 million (approximately US$1.6 million); by 2017, this had grown to around £3.2 million (approximately US$3.9 million).[40]

[34] House of Commons DCMS Committee, supra note 31.

[35] Id. ¶ 14.

[36] Id. ¶ 13.

[37] Id.

[38] Id.

[39] Ofcom, *Addressing Harmful Online Content*, supra note 8, at 2.

[40] DCMS Committee, supra note 31, ¶ 200.

There are no laws specifically designed to regulate online political advertisements, but the current law[41] does regulate how much money[42] political parties[43] and candidates[44] may spend on their election campaigns during the regulated period prior to an election.[45] The focus on digital advertisements in Great Britain in relation to the current electoral financing laws is to ensure that any costs and expenditure connected with producing and/or disseminating digital materials are appropriately recorded and reported, if they fall within the regulated period.[46] Any spending outside of this period is not regulated[47] and there are concerns that political advertisements disseminated outside of this period are used to influence the political debate across the UK.[48]

No specific category exists under which spending on digital advertisements must be recorded. Digital spending frequently falls under the broad category of advertising, and the Electoral Commission has recommended that spending categories should be revised and subheadings added to include the type of medium or format used, along with more detailed invoices for digital advertisements,[49] to "provide more useful information about what campaigners have spent money on."[50]

Digital advertisements that target specific segments of the population through demographic factors such as age, gender, or location—commonly referred to as "dark ads"—is currently legal. The Electoral Commission has noted that the law is unclear as to the amount of detail that should be included when reporting this type of expenditure, and there do not appear to be any requirements for the disclosure of any data as to the content of these ads or the demographic the ads are targeting.[51] The Electoral Commission has recommended that campaigners should

[41] Representation of the People Act 1983, c. 2, https://perma.cc/D2QN-NKE9; Political Parties, Elections and Referendums Act 2000, c. 41, https://perma.cc/CL4C-FEY8; Political Parties and Elections Act 2009, c. 12, https://perma.cc/E4HK-BRP8.

[42] The definition of campaign expenditure for political parties extends to party political broadcasts, advertising of any nature, unsolicited material addressed to electors, manifesto or other policy documents, market research or canvassing, media/publicity, transportation, and rallies or other events. Political Parties, Elections and Referendums Act 2000, c. 41, sched. 8 ¶ 1.

[43] The limit on campaign expenditures by a party in a parliamentary general election is either a set amount in each part of the UK and is currently either £810,000 (about US$985 million) in England, £120,000 (about US$146,000) in Scotland, £60,000 (about US$73,000) in Wales, or £30,000 (about US$36,000) multiplied by the number of constituencies (seats) contested by the party in that part of the UK, whichever is greater. Id. sched. 9, ¶ 3(2) & (3).

[44] Id. c. 41, Pt. IV. § 71A & sched. 2A.

[45] Id.; Representation of the People Act 1983, c. 2 § 72 & sched. 9.

[46] See, e.g., *Code of Practice: Political Parties (Current Draft)*, Electoral Commission, https://perma.cc/79KL-GK4L.

[47] Stephen Adshead et al., *Online Advertising in the UK (*Jan. 2019), https://perma.cc/MJ5V-9GVT.

[48] Equality and Human Rights Commission, supra note 14 at 16.

[49] Electoral Commission, *Digital Campaigning: Increasing Transparency for Voters* ¶ 103, https://perma.cc/C3T8-Z875.

[50] *Spending on Digital Campaign Activity*, The Electoral Commission, https://perma.cc/6WKQ-8EST.

[51] Id.

provide "meaningful information about the details of their campaigns . . . [including] the messages used in those campaigns, which parts of the country they were targeted at, and how much was spent on each campaign."[52]

The Electoral Commission has provided further guidance on the application of this law to digital materials and advertisements, stating as follows:

> The rules do cover the costs of placing adverts on digital platforms or websites. They include the costs of distributing and targeting digital campaign materials or developing and using databases for digital campaigning. This applies even if the original purchase of hardware or software materials falls outside the regulated period for reporting spending. Spending limits and rules to report spending apply to campaign spending on advertising. The same rules apply whether campaigners use long-standing techniques, such as printed mailshots or billboards, or newer ones, such as emails and online adverts.[53]

Some skillfully drafted campaign ads result in supporters sharing the message via social media with friends and family. This is known as the "organic" reach and is not covered by the current electoral spending rules. The Electoral Commission has stated that while it will continue to consider the question of regulating electoral campaigns in different ways, the current focus will remain on the money spent on campaigns and that the organic reach of these particular ads "is not different from more traditional forms of campaigning, where some campaigners are more effective than others."[54]

As noted above, the Electoral Commission has stated that while there is a general principle in Great Britain that funding from overseas is not permitted, "the rules do not explicitly ban overseas spending"[55] and were written to address concerns that foreign nationals would donate money to political parties. At the time the law was drafted, the government "had not seen the potential for foreign sources to directly purchase campaign advertising in the UK."[56] This has meant that foreign nationals who would be unable to register as third-party campaigners[57] in Great Britain are able to purchase digital advertisements in their home country and target voters in Great Britain.[58]

D. Proposals to Regulate Online Political Advertisements

Current electoral law has been described as "not fit for purpose"[59] due to the move to online and micro-targeted campaigning. The Electoral Commission has made a number of recommendations

---

[52] Id.

[53] Id.

[54] Id.

[55] Id.

[56] *Who Pays for Digital Campaigns*, The Electoral Commission, https://perma.cc/TLF7-39YT.

[57] *Non-Party Campaigners*, The Electoral Commission, https://perma.cc/U2XE-78VV.

[58] Id. ¶ 86. See also DCMS Committee, supra note 31, ¶ 267.

[59] DCMS Committee, supra note 31, ¶ 211.

of changes that should be made to ensure that digital campaigns follow the UK's electoral rules, are transparent, and prevent foreign funding of election and referendum campaigns.[60] The Electoral Commission has recommended that the government

- introduce legislation to specifically prohibit campaign spending from overseas;
- update the law to require any digital campaign material to have an imprint that states who created and funded the campaign;
- increase transparency by requiring more detailed invoices for digital advertisements from political parties, candidates, and third-party campaigners;[61] and
- increase the investigatory powers of the Electoral Commission, and the maximum fine (currently £20,000, approximately US$25,000) that the Electoral Commission can levy on campaigners that break the rules.[62]

The Electoral Commission has also expressed concern that the compilation of datasets and databases utilized for targeted digital advertisements may occur before the regulated period and thus fall outside the expenditure and reporting period for political parties, candidates, and registered third-party campaigners. It has recommended that parties and candidates should declare an estimate of any expenditure the party or candidate has invested in purchasing or developing any data held at the time of registration as a party or candidate.[63]

These recommendations have been repeated by a number of reports and public bodies, including the Committee on Standards in Public Life[64] and the DCMS Committee, which has called for the government to

> review[] the current rules on overseas involvement in our UK elections to ensure that foreign interference in UK elections, in the form of donations, cannot happen. We also need to be clear that Facebook, and all platforms, have a responsibility to comply with the law and not to facilitate illegal activity.[65]

The DCMS Committee has recommended that current electoral legislation be updated to take into account current technology and include provisions that are "explicit on the illegal influencing of the democratic process by foreign players."[66] The DCMS Committee called for electoral law to cover all political campaigning, include a legal definition of what constitutes digital campaigning

[60] Electoral Commission, *Digital Campaigning: Increasing Transparency for Voters*, supra note 49.

[61] Id. ¶ 103.

[62] *Spending on Digital Campaign Activity*, The Electoral Commission, supra note 50.

[63] Electoral Commission, *Digital Campaigning: Increasing Transparency for Voters*, supra note 49, ¶ 86.

[64] *Improvements Are Needed to Ensure Transparency for Voters in a Digital Age*, Committee on Standards in Public Life (June 28, 2018), https://perma.cc/76XV-VLW6.

[65] DCMS Committee, supra note 31, ¶ 267.

[66] Id. ¶ 249.

and online political advertising, and require clear banners on all political advertisements and videos that identify the source of advertising and the advertiser.[67]

The government responded to these recommendations and, in May 2019, announced its intention to introduce a "digital imprint regime" for digital advertisements later in the year.[68] The proposed regime will be similar to the imprints required for printed electoral advertisements, which require information on who printed the document, who promoted the material, and the person for whom the material is being published.[69] There is uncertainty at this stage over which forms of digital election material will be included—for example, whether it would extend to sponsored posts from online "influencers" or advertising via emails and social media.[70] The government has stated that it will retain[71] the definition of "election material" contained in the Political Parties, Elections and Referendums Act 2000, which reads as follows:

> "Election material" means material which can reasonably be regarded as intended to promote or procure electoral success at any relevant election for—
> (a) one or more particular registered parties,
> (b) one or more registered parties who advocate (or do not advocate) particular policies or who otherwise fall within a particular category of such parties, or
> (c) candidates who hold (or do not hold) particular opinions or who advocate (or do not advocate) particular policies or who otherwise fall within a particular category of candidates.[72]

The government has expressed concern that any measures introduced should not be overly burdensome to implement and enforce.[73] It has also stated that any measures should not interfere with members of the public engaging in a full democratic debate. For example, it considers that requiring individuals sharing information for personal reasons to include an imprint could deter them from sharing election material and thus limit democratic engagement.[74] The government has stated that it "will think very carefully about how we might introduce a digital imprints regime that provides greater transparency for voters, but does not adversely affect democratic engagement or stifle healthy debate."[75]

The Electoral Commission is currently drafting a Code of Practice on electoral spending for political parties and candidates, which will require that specified costs of producing and disseminating digital or electronic advertising material—including for such things as designing,

---

[67] *Democracy Is at Risk*, supra note 33.

[68] Cabinet Office, *Protecting the Debate: Intimidation, Influence and Information Government Response* (2019), https://perma.cc/NG38-Y9UZ.

[69] Id. at 11.

[70] Id. at 32-37

[71] Id. at 33.

[72] Political Parties, Elections and Referendums Act 2000, c. 41 § 143A.

[73] Cabinet Office, *Protecting the Debate: Intimidation, Influence and Information Government Response*, supra note 68.

[74] Id. at 37.

[75] Id. at 36.

developing, and disseminating material; paying for a more prominent position within a search engine; and web hosting—should be counted as electoral spending.[76]

III. Government Actions

A. Fusion Doctrine

In the wake of Russian disinformation after the poisoning of Sergei Skripal and others in England,[77] the government "judged the Russian state promulgated at least 38 false disinformation narratives around this criminal act."[78] The Prime Minister announced that the intelligence services would be responsible for identifying social media platforms that distribute misinformation and disinformation under the Fusion Doctrine, which was introduced as a central part of the March 2018 National Security Capability Review.[79] This doctrine provides the

> Government must use the full suite of security, economic, diplomatic and influence capabilities to deliver our national security goals. This means strategic communications are to be considered with the same seriousness as financial or military options.[80]

Former Prime Minister Theresa May did not detail how the Fusion Doctrine will apply to mis- and disinformation online.[81] The government's response to a citizen's Freedom of Information request revealed that little information on the Fusion Doctrine has been made available to either Members of Parliament or the press beyond what is contained in the National Security Capability Review.[82]

B. National Security Communications Team

Following the influx of misinformation and disinformation campaigns, in April 2018 the government announced that it would "significantly expand" the National Security Communications Team (NSCT).[83] The purpose of the NSCT is to tackle communications elements of threats to national security, including (but not limited to) disinformation.[84] It is staffed by the

---

[76] *Code of Practice: Political Parties (Draft)*, Electoral Commission, ¶¶ 2.13, 3.1-3.10, https://perma.cc/3QUK-68FH.

[77] PM Statement to Parliament on the Salisbury Investigation, Prime Minister's Office, 10 Downing Street and The Rt Hon Theresa May MP (Sept. 5, 2018), https://perma.cc/6N7G-ADKC.

[78] House of Commons DCMS Committee, supra note 7, at 16.

[79] HM Government, supra note 2, at 10-11.

[80] Alex Aiken, *Disinformation Is a Continuing Threat to Our Values and Our Democracy*, Government Communication Service Blog (June 12, 2018), https://perma.cc/CJ8H-JKXB.

[81] 638 Parl. Deb. HC (2018) (6th ser.) 45WS (2018), https://perma.cc/5V2D-X7AW.

[82] Letter to Mike Robinson from FOI Team, Cabinet Office (Apr. 19, 2018), https://perma.cc/YJ3J-4AQL.

[83] Id.

[84] Cabinet Office, *Mass Media: Standards: Written Question – 134225,* Parliament.UK (May 10, 2018), https://perma.cc/RNL4-FQWE.

Government Communication Service, the professional body for people working in communications roles across the UK government.[85]

Few details have been provided about the NSCT beyond the announcement that it would be expanded, and that announcement did not reference misinformation or access to balanced information.[86] Government answers to a series of written parliamentary questions on the NSCT have given little detail on how the NSCT operates.[87] A spokesperson for then Prime Minister Theresa May outlined that the NSCT would "be tasked with combating disinformation by state actors and others. It will more systematically deter our adversaries and help us deliver on national security priorities."[88]

The NSCT has implemented a "Don't Feed the Beast" campaign which highlights ways the public can spot disinformation before it is spread.[89] Examples of disinformation provided by the campaign include false claims about vaccinations, false accusations of rioting, and hoax stories.[90]

The campaign uses the "SHARE checklist" to help the public form an opinion about the reliability of online information:

> **Source**
> Make sure that the story is written by a source you trust, with a reputation for accuracy. If it's from an unfamiliar organisation, check for a website's 'About' section to learn more.
>
> **Headline**
> Always read beyond the headline. If it sounds unbelievable, it very well might be. Be wary if something doesn't seem to add up.
>
> **Analyse**
> Make sure you check the facts. Just because you have seen a story several times, doesn't mean it's true. If you're not sure, look at fact checking websites and other reliable sources to double check.
>
> **Retouched**
> Check whether the image looks like it has been or could have been manipulated. False news stories often contain retouched photos or re-edited clips. Sometimes they are authentic, but have been taken out of context.

[85] HM Government, supra note 2, at 34.

[86] 638 Parl. Deb., supra note 81.

[87] See, e.g., Cabinet Office, *National Security Communications Unit: Written Question – 126982*, Parliament.UK (Feb. 12, 2018), https://perma.cc/BWJ3-9AUG; Cabinet Office, *National Security: Written Question – 124854*, Parliament.UK (Mar. 16, 2018), https://perma.cc/L8RH-LSXG.

[88] William James & Elizabeth Piper, *Britain to Set Up Unit to Tackle 'Fake News' – May's Spokesman*, Reuters (Jan. 23, 2018), https://perma.cc/2N7U-Q5MH; *Government Announces Anti-Fake News Unit*, BBC News (Jan. 23, 2018), https://perma.cc/2DCV-G472.

[89] *Don't Feed the Beast*, HM Government, https://perma.cc/2U57-MU5Q.

[90] Id.

> **Error**
> Many false news stories have phony or look-alike URLs. Look out for misspellings, bad grammar or awkward layouts.[91]

The campaign aims to increase public resilience to disinformation, by educating and empowering "those who see, inadvertently share and are affected by false and misleading information."[92]

C. Rapid Response Unit

While the regulatory approach to countering misinformation is currently under consideration, in the wake of a series of false stories posted online that were damaging to the Conservative Party and the government[93] the Cabinet Office established a Rapid Response Unit in April 2018 to help the government meet its policy of "reclaiming a fact-based public debate."[94]

The Rapid Response Unit operates from within the executive branch of the government and is comprised of "specialists including analyst-editors, data scientists, media and digital experts."[95] The Unit is part of the Government Communications Service (GCS) and based in government headquarters at No. 10 Downing Street and the Cabinet Office.[96] The Unit's funding was extended in early 2019 following the successful pilot started in April 2018.[97]

The role of the Rapid Response Unit is to "monitor[] news and information being shared and engaged with online to identify emerging issues with speed, accuracy and with integrity."[98] The results of this monitoring "helps government understand the current media environment and assess the effectiveness of their public communications."[99]

The Rapid Response Unit has developed a model with the acronym FACT to help it identify and respond to misleading online content:

> **Find**: Constantly monitor online news sources and publicly available social media posts to identify themes/discussions/stories that promote false and misleading information relating to HMG [Her Majesty's Government]. This may be misinformation or disinformation.

---

[91] Id.

[92] Id.

[93] Francis Elliot, *Whitehall's Online Rapid Response Unit Will Block Fake News*, The Times (London) (Jan. 20, 2018) (available by subscription), https://perma.cc/CX64-EZX9.

[94] *Alex Aiken Introduces the Rapid Response Unit*, Government Communication Service (July 19, 2018), https://perma.cc/837J-UF2U.

[95] Id.

[96] Cabinet Office, *Mass Media: Standards: Written Question – 134225*, supra note 84.

[97] Cabinet Office, *Rapid Response Unit: Written Question – 226754*, Parliament.UK (Mar. 4, 2019), https://perma.cc/KL7K-MBTL.

[98] *Alex Aiken Introduces the Rapid Response Unit*, supra note 94.

[99] Government Communication Service, supra note 9, at 9.

> **Assess**: Assess the scale of engagement with the risk identified and establish whether it is appropriate to respond to the content. Flag to relevant press offices and advisors, with a recommended approach to response. This is almost never direct rebuttal.
> **Create**: Create appropriate content with the aim of rebalancing the narrative and promoting official HMG information. This may be a press office line, a social media post, or the creation of a new asset.
> **Target**: Target content to ensure HMG information is highly visible and accessible to the public.[100]

The aim of the FACT model is to "empower[] media and digital officers with the tools to respond to inaccuracies at speed."[101] The government has emphasized that the Rapid Response Unit is not a rebuttal, or "fake news" unit.[102] Instead, it focuses on checking trends in new sources and, where certain search terms indicate a bias in results, it works to optimize government pages to appear higher in search results or will activate social media content to help "rebalance the narrative and reassure those who were most engaged with the topic."[103] The Unit does not store any information on social media accounts that share misinformation and disinformation.[104] An example provided by the government demonstrates action the Rapid Response Unit took after it detected misinformation:

> [F]ollowing the Syria airstrikes, the unit identified that a number of false narratives from alternative news sources were gaining traction online. These "alt-news" sources are biased and rely on sensationalism rather than facts to pique readers' interest.
>
> Due to the way that search engine algorithms work, when people searched for information on the strikes, these unreliable sources were appearing above official UK government information. In fact, no government information was appearing on the first 15 pages of Google results. We know that search is an excellent indicator of intention. It can reflect bias in information received from elsewhere.
>
> The unit therefore ensured those using search terms that indicated bias— such as 'false flag'—were presented with factual information on the UK's response. The RRU improved the ranking from below 200 to number 1 within a matter of hours. Information on UKAID's work in the region was also immediately amplified amongst audiences demonstrating the highest levels of interest in humanitarian issues affecting displaced Syrians.[105]

The Rapid Response Unit works closely with the NSCT, particularly in times of crisis, to provide highly visible public information.[106] Examples of this action include countering misinformation on the origin of the nerve agent used to poison former Russian operatives in England, and the

---

[100] Id. at 7.

[101] HM Government, *Government Communication Plan 2019/2020* (2019), at 19, https://perma.cc/7H4K-UHCW.

[102] *Alex Aiken Introduces the Rapid Response Unit*, supra note 94.

[103] Id.

[104] Cabinet Office, *Mass Media: Internet: Written Question - 164285,* Parliament.UK (July 19, 2018), https://perma.cc/7C3D-9MGF.

[105] Id.

[106] Government Communication Service, supra note 9, at 9.

implementation of targeted digital communications to audiences during military action in Syria.[107]

In addition to monitoring misinformation, the Rapid Response Unit acts to ensure government communications are impactful, promoting a "fact-based public debate."[108] This includes coordinating with media teams across government to ensure they are equipped to quickly and effectively respond to the modern news environment, including mis- and disinformation.[109] This includes responding to stories on domestic issues, such as the health service and crime.[110]

D. The RESIST Model – For Government Departments

Tackling misinformation and disinformation forms part of the "Strengthening Democracy" strand of the Government Communication Plan 2019/20.[111] The RESIST model for tackling disinformation was established in March 2018.[112] It was designed to provide government departments with the ability to create long-term and strategic responses to disinformation.[113] RESIST lies within the NSCT's broader objective to further integrate communications into national security strategy and decision-making, in line with the FUSION doctrine.[114]

The RESIST model stands for the following six principles:

Recognise disinformation
- What are the objectives of disinformation?
- What are the techniques of disinformation?
- How does disinformation combine techniques to achieve an impact?

Early warning
- How do I focus digital monitoring on my priorities?
- How do I build a digital monitoring toolbox?
- How can I use digital monitoring to assess potential threats and vulnerabilities?

Situational insight
- What is the insight in the context of disinformation and how should it be used to support a timely response to disinformation?

[107] Id.

[108] Cabinet Office, *Rapid Response Unit: Written Question – 226754*, supra note 97.

[109] Id.

[110] Chloe Smith, Cabinet Office, *Mass Media: Internet: Written Question – 157646,* Parliament.UK (July 2, 2018), https://perma.cc/QNM3-8RKW.

[111] HM Government, *Government Communication Plan 2019/2020*, supra note 101, at 18-21.

[112] Id. at 20.

[113] Id. at 19.

[114] Id. at 20.

Impact analysis
- What is the likely goal of the disinformation?
- What is the likely impact of the disinformation?
- What is the likely reach of the disinformation?
- How should I prioritise the disinformation?

Strategic communication
- What should a public response to disinformation look like?
- What is the sign-off process?
- What are the available options for responding?

Track outcomes
- How should I record and share information about the disinformation campaign?
- How can I evaluate my actions and understand the lessons learned? [115]

The RESIST model is designed to complement the FACT model by "providing departments with the means to create a long-term strategic response to disinformation."[116]

IV. Media Coordination

A. Traditional Broadcast Media

1. Misinformation

The traditional broadcast media operate under a legislative framework and a Broadcasting Code, which the government has noted could be used as a model for the regulation of tech companies to counter the publication and spread of misinformation and disinformation.[117] The Communications Act 2003 and Broadcasting Acts of 1990[118] and 1996[119] provide the legislative framework within which broadcasters operating in the UK must operate.[120] Ofcom was established under the Communications Act 2003 and has a number of roles, including enforcing content standards across television and radio broadcasters and the UK's media and telecommunications companies.[121] When carrying out its statutory functions, Ofcom has a duty to ensure that television and radio services have

[115] Id.

[116] Id. at 19.

[117] DCMS Committee, supra note 31, ¶ 38.

[118] Broadcasting Act 1990, c. 42, https://perma.cc/M4B2-RXVP.

[119] Broadcasting Act 1996, c. 55, https://perma.cc/R9VN-8ER2.

[120] Web content, even when provided on broadcasters' websites, is not regulated by Ofcom. Mike Dodd & Mark Hanna, *Essential Law for Journalists* ¶ 3.3 (23rd ed. 2016).

[121] Id.

> . . . standards that provide adequate protection to members of the public from the inclusion of offensive and harmful material in such services [and that] provide adequate protection to members of the public and all other persons from both:
> (i) unfair treatment in programmes included in such services; and
> (ii) unwarranted infringements of privacy resulting from activities carried on for the purposes of such services.[122]

In order to provide television, radio, or on-demand video services in the UK, broadcasters must obtain a license from Ofcom under the Broadcasting Act 1990 and Broadcasting Act 1996. In order to grant a license, Ofcom examines the application to determine whether the applicant and the proposed programming are "fit and proper."[123] If it considers that these criteria are met it may grant the license for a set duration, which may be renewed. State-controlled broadcasters that are licensed by Ofcom are required along with other broadcasters to comply with the Broadcasting Code.[124]

Section 3(4)(g) of the Communications Act 2003 requires Ofcom to protect audiences against harmful and offensive material "in the manner that best guarantees an appropriate level of freedom of expression."[125] Working together, the Communications Act 2003 and the Broadcasting Act 1996 place a duty on Ofcom to establish the standards for broadcasts, and compliance with these standards is part of the license conditions imposed on broadcasters.[126]

The Broadcasting Code contains various rules, including those

- prohibiting the broadcast of materials likely to incite crime or disorder;[127]
- ensuring that news reports are provided with due accuracy and due impartiality,[128] with the Broadcasting Code notably specifying that, "[i]n dealing with matters of major political and industrial controversy and major matters relating to current public policy an appropriately wide range of significant views must be included and given due weight in each programme or in clearly linked and timely programmes," and "[v]iews and facts must not be misrepresented";[129]

[122] Id. § 3(2).

[123] Broadcasting Act 1990, c. 42 § 3(3); Broadcasting Act 1996, c. 55 § 3(3).

[124] Ofcom, *Update on the Rt Service – New Broadcasting Investigations and Approach to Fit & Proper* ¶ 16, https://perma.cc/X9WV-CKM7.

[125] Communications Act 2003, c. 21 § 3(4)(g).

[126] Ofcom, *The Ofcom Broadcasting Code* (Apr. 2017), https://perma.cc/7UAS-MA84.

[127] Id. at 21; Communications Act 2003, c. 21 § 319(2)(b).

[128] *The Ofcom Broadcasting Code*, supra note 126, at 28; Communications Act 2003, c. 21 §§ 319(2)(c)-(d), 319(8), 320.

[129] *The Ofcom Broadcasting Code*, supra note 126, ¶ 5.12.

- avoiding unfair or unjust treatment of individuals or organizations within programming;[130] and
- ensuring broadcasters maintain editorial independence and control over programing.[131]

If a broadcaster breaches the Code, Ofcom publishes its findings explaining why the broadcaster breached the Code and may direct that the program not be repeated, or order the broadcaster to air a correction or statement of its findings. If a broadcaster breaches the Code in a serious, deliberate, or repeated manner, Ofcom may impose statutory sanctions against the broadcaster, including fines of up to £250,000 (approximately US$318,000) or 5% of the broadcaster's revenue, and it may shorten, suspend, or revoke the broadcaster's license.[132]

2. Political Advertisements

Political advertisements through traditional broadcast media are prohibited,[133] and this has "been held to be a justifiable interference with the rights of campaigning groups to free expression."[134] Political parties receive a certain amount of broadcasting time on national television and radio free of charge.[135] The formula for the allocation, length, and frequency of party political broadcasts is determined by the independent communications regulator Ofcom[136] for commercial broadcasters with public service obligations and, for the 2016 elections, the minimum allocation of party electoral broadcasts was four minutes and forty seconds.[137] This time was rarely exceeded. The British Broadcasting Corporation's charter agreement contains a provision that it will carry party political broadcasts, subject to the requirements imposed by Ofcom.[138]

[130] Id. ¶ 7.1.

[131] Id. ¶ 9.1; Communications Act 2003, c. 21 § 319(2)(j).

[132] *The Ofcom Broadcasting Code*, supra note 126, ¶ 9.1.

[133] Communications Act 2003, c. 21, § 333. See also Advertising Standards Agency, *The BCAP Code: The UK Code of Broadcast Advertising* ch. 7, https://perma.cc/6L6V-F3QG.

[134] Equality and Human Rights Commission, supra note 14, at 16.

[135] Communications Act 2003, c. 21, § 333.

[136] Ofcom, *Guidance Notes Section Six: Elections and Referendums* (Mar. 2017), https://perma.cc/WA5S-6KRU.

[137] *Statement on Party Election Broadcast Regulations,* Ofcom (Mar. 11, 2016), https://perma.cc/79VU-MSLL. The current rules are available at *Ofcom Rules on Party Political and Referendum Broadcasts*, Ofcom (Mar. 22, 2017), https://perma.cc/69LN-ZL5Z. Guidance to assist broadcasters on how Ofcom usually interprets and applies the Broadcasting Code and its rules is found in *Ofcom Guidance Notes*, *Section 6: Elections and Referendums*, Ofcom (Mar. 22, 2017), https://perma.cc/B2AS-NHHV.

[138] Department for Culture, Media and Sport, Broadcasting: An Agreement Between Her Majesty's Secretary of State for Culture, Media and Sport and the British Broadcasting Corporation, 2016, Cm. 9366, at 58, https://perma.cc/HTJ3-W47Q.

B. Online Media

1. Misinformation

As noted above, there are currently no specific laws that prohibit the publication of misinformation or disinformation online. The government has been investigating the impact of this type of information and has published number of reports on the subject, discussed above. The government has expressed frustration with respect to the failure of top Facebook officials to respond to inquiries. In 2018, Mark Zuckerberg failed to appear before the DCMS Committee,[139] despite several invitations,[140] and did not respond personally to any of the correspondence with the Committee.[141] After failing to appear before the Committee, Zuckerberg was invited three times to speak in front of an "international grand committee" in Parliament, which grew to include representation from nine countries, but these invitations were also refused.[142] The DCMS Committee wrote in their *Disinformation and 'Fake News': Final Report* that Zuckerberg had acted in contempt of Parliament for not appearing before them and not responding in person.[143]

2. Political Advertisements

Unlike traditional broadcast media, there are currently no restrictions on political advertising on digital platforms. A number of social media companies have announced their intention to make political ads more transparent, including across the UK. The Electoral Commission has reported that Facebook, Google, and Twitter intend to take steps to include labels showing who has paid for digital ads on their platforms, and that they will publish online databases of the political ads that they have been paid to run, along with information about who was targeted by the advertisements, the reach, and amount spent.[144]

There are no restrictions on the content of political advertisements. Commercial advertisements are regulated by the Advertising Standards Agency, which enforces a strict set of standards that must be met by advertisers across the UK.[145] These standards do not apply to digital political advertisements.

---

[139] Letter from Damian Collins, Chair, DCMS Committee, House of Commons, to Mark Zuckerberg, CEO, Facebook (Mar. 20, 2018), https://perma.cc/TDA7-4A54.

[140] Letter from Damian Collins, Chair, DCMS Committee, House of Commons, to Rebecca Stimson, Head of Public Policy, Facebook UK (May 1, 2018), https://perma.cc/VC3K-9N5B.

[141] DCMS Committee, supra note 31, ¶ 29.

[142] Id.

[143] Id.

[144] Electoral Commission, *Digital Campaigning Increasing Transparency for Voters*, supra note 49, ¶¶ 55-58.

[145] Guy Parker, *Most Political Players Shun Ad Standards that Big Companies Sign-up to*, ASA Blog Post (July 5, 2016), https://perma.cc/4BHX-Z7DV.

In October 2018, Facebook introduced steps aimed to prevent foreign advertising within the UK on political causes, expanding a system already in place in the US and Brazil.[146] To run ads that "reference political figures, political parties, elections, legislation before Parliament and past referenda that are the subject of national debate"[147] on Facebook or a linked Instagram page, the individual must prove that he or she is based in the UK using identification such as a passport, and that the advertisements will display a "paid for by" disclaimer. The "paid for by" disclaimer is a clickable link that takes users to the Ad Library provided by Facebook that will include information about the range of the advertisement's budget and how many people it has reached, and list any other ads that the page is running. These advertisements are then stored for up to seven years in a public, searchable Ad Library, which is accessible to anyone, including those without a Facebook account.[148] These steps have been criticized as not being transparent and as "no substitute for publicly accountable regulation."[149]

Twitter has yet to take any UK-specific steps to prevent political advertising from overseas during elections.

[146] *Bringing More Transparency to Political Ads in 2019*, Facebook Business (Jan. 15, 2019), https://perma.cc/C42E-F669.

[147] Richard Allan & Rob Leathern, *Increasing Transparency for Ads Related to Politics in the UK*, Facebook Newsroom (Oct. 16, 2018), https://perma.cc/K386-4AGM.

[148] *Facebook Ad Library*, Facebook, https://perma.cc/P42L-URH8.

[149] London School of Economics and Political Science, *Tackling the Information Crisis: A Policy Framework for Media System Resilience* (undated), https://perma.cc/5Z7S-FJU7.