PRIVACY VS. POLITICAL INTEGRITY: HOW EUROPEAN DATA PROTECTION LAWS MAY LIMIT THE REGULATION OF FOREIGN POLITICAL INTERFERENCE IN U.S. ELECTIONS

Elvira Sihvola*

U.S. elections have seen an unprecedented amount of foreign interference in recent years. In a world where a growing amount of political advertising happens online, this interference also increasingly occurs on the Internet. Revelations of Russian election meddling in the 2016 election cycle through social media platforms has led American lawmakers and other stakeholders to attempt to address the issue in a variety of ways, including by instating new laws on online advertising and industry-led efforts to reform transparency practices online. At the same time, the European Union has embarked on an ambitious effort to overhaul the regulation of data protection and privacy on the internet by introducing the Global Data Protection Regulation ("GDPR"), set to take effect in 2019. The impacts of this regulatory overhaul extend well beyond the European Union, impacting the practices of global technology companies and cross-border data transfers. This note discusses the effects of the GDPR on American attempts to regulate interference in U.S. elections, by examining the European data protection framework, American efforts to regulate foreign election interference, and evaluating how these two phenomena interact. The note argues that the requirements of EU’s data protection framework may limit the effectiveness of American regulatory efforts by setting strict protections on the privacy of user data. It calls for greater harmonization of data protection laws globally to better meet the increasingly global nature of data flow and online activity.

INTRODUCTION ........................................................................................................137

PART I ................................................................................................................... 139

Regulatory Frameworks: Data Protection and Political Advertising ......139
A. European Data Protection Framework...............................................139
   i. Fundamental Rights.................................................................139
   ii. Data Protection Directive....................................................140
   iii. US-EU Safe Harbor Agreement..........................................141
   iv. The General Data Protection Regulation.........................141

* Columbia Law School, J.D. Candidate, 2019.
v. ECJ Case Law: Schrems v. Data Protection Commissioner ........................................ 142
vi. EU-US Privacy Shield ......................................................... 143
vii. Challenges to Privacy Shield and Third Country Data Transfers ........................................ 144

B. U.S. Regulation of Online Political Advertising ...................... 146
i. FEC Regulation of Online Advertising .................. 146
ii. Federal Communications Commission Transparency Requirements ...................................... 148
iii. Political Activity by Foreign Nationals ....................... 148

PART II .............................................................. 149

Proposed Legislation to Address Foreign Interference in US Elections . 149
A. U.S. Policy Proposals to Address Foreign Political Advertising ........................................ 149
   i. Honest Ads Act .......................................................... 149
   ii. We the People Democracy Reform Act .................. 150
   iii. FEC Proposed Rulemaking on Internet Communication Disclaimers .................................. 150
   iv. Industry Self-Regulation .............................................. 151

PART III .............................................................. 153

European Data Protection and US Legislative Efforts ...................... 153
A. Legislative Proposals in light of European Data Protection Framework ........................................ 153
   i. Territorial Reach of the GDPR .................. 154
   ii. Third Country Data Transfers under the GDPR ........ 155
   iii. GDPR Derogations for Specific Purposes ............... 156
   iv. Consent and Confidentiality of Personal Data .......... 157
B. Online Political Advertising Policy Proposals and European Data Protection .................. 157
   i. Honest Ads Act and We the People Act ............... 157
   ii. FEC Rulemaking ...................................................... 158
   iii. Industry Self-Regulation .......................................... 158

PART IV .............................................................. 159

Implications of European Data Protection Regulations and The Way Forward ........................................ 159
   i. Privacy Interests at Stake ............................................ 159
   ii. Third Country Transfers .............................................. 160
   iii. Personal Data about Natural vs. Legal Persons ........ 162
   iv. Issue vs. Candidate-Specific Ads ...................... 162
   v. Impact on Third Country Nationals .............. 162
   vi. U.S. Criminal Enforcement .................. 163
   vii. EU Enforcement ...................................................... 165
   viii. Conflict of EU and U.S. Laws ....................... 165
   ix. Harmonization of Data Protection Globally .......... 166
   x. Implications for Regulation of Fake News .......... 167

CONCLUSION .............................................................. 168
INTRODUCTION

During the 2016 U.S. election cycle, foreign entities and individuals attempted to interfere with U.S. elections by disseminating misleading information and purchasing political advertisements on various online platforms.¹ On Facebook alone, accounts linked to Russian entities and individuals purchased thousands of ads between June 2015 and May 2017.² Similar patterns of foreign interference have been reported in connection with the 2018 midterm elections.³ In light of these revelations concerning foreign interference,⁴ advocates have called for the Federal Election Commission to re-evaluate and renew its regulation of online political advertising.⁵ Multiple stakeholders have raised transparency concerns over the identity of foreign actors responsible for funding misleading political advertisements on social media platforms. In response, two bipartisan bills propose to reform the regulation of online political advertising.⁶ Additionally, in the face of public scrutiny, technology companies such as Facebook and Twitter have offered to share information about foreign actors with United States (“U.S.”) regulators,⁷ and to continue their practice of industry self-regulation.⁸

However, the sharing of this important information about foreign actors with U.S. regulators is restricted under the European Union’s (“EU”) data privacy regime. This

regime is currently more extensive than the U.S. data protection framework.\(^9\) The EU allows transfers of data only to countries that it deems to have strong data protections in place,\(^10\) such as Argentina, Switzerland, and New Zealand.\(^11\) In 2015, the European Court of Justice struck down a data transfer framework between the U.S. and the EU that allowed companies to move digital information about user data across the Atlantic.\(^12\) It found that the framework allowed the U.S. government to interfere with the fundamental rights of persons whose data was, or could be, transferred from the EU to the U.S. This was a result of the framework’s extensive exception on national security, public interest, and U.S. domestic legislation grounds. In response, the EU and U.S. negotiated a new data transfer agreement, the EU-U.S. Privacy Shield, to remedy some of the legal problems in the prior agreement. However, critics such as European privacy activists,\(^13\) an EU working group overseeing data protection,\(^14\) and members of the European Parliament,\(^15\) remain unsatisfied with the level of protection the new data transfer agreement provides. Moreover, the EU recently enacted a new General Data Protection Regulation to replace its previous data protection legislation, which includes extensive user protection provisions.\(^16\) This may further complicate the transfer of data to the U.S.

This Note argues that the EU’s data protection framework may limit the effectiveness of American attempts to regulate foreign interference in U.S. elections, and calls for greater harmonization of internet regulations globally. Part I begins with

---


\(^12\) Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 EUR-Lex CLEX LEXIS 650 (Oct. 6, 2015), ¶ 87.

\(^13\) See Max Schrems, The Privacy Shield is a Soft Update of the Safe Harbor, 2 EUR. DATA PROT. L. REV. 148, 148–49 (2016) (arguing that the new Privacy Shield does not go far enough to protect European Union fundamental rights).


\(^16\) Aliya Ram & Hannah Kuchler, Europe’s Data Rule Shake-Up: How Companies Are Dealing with It, FIN. TIMES, (Jan. 3, 2018), https://www.ft.com/content/60e9c680-e17d-11e7-a8a4-0a1e63a52f9c [https://perma.cc/M36T-QJXN].
an examination of the European data protection framework, the European-American data transfer agreements, and recent European Court of Justice case law emphasizing the fundamental right to privacy and personal data in the context of data transfers to third countries. It also provides a summary of the current American framework for regulating online political advertising. Part II provides an overview of the proposed legislation for the regulation of foreign interference in U.S. elections through political advertising. It also describes alternative available measures, such as industry self-regulation. Part III considers how the European data protection framework, especially the new General Data Protection Regulation and EU-U.S. Privacy Shield, will affect American efforts to regulate foreign political advertising. Part IV explores the privacy interests at stake, as well as the implications posed by EU data protection rules for companies and regulators in this context. It then points out gaps left in the framework, including concerns with criminal enforcement, issue vs. candidate-specific ads, conflicts of law, and so-called fake news.

PART I

Regulatory Frameworks: Data Protection and Political Advertising

A. European Data Protection Framework

The EU has one of the most extensive data protection regimes in the world. The protections offered through this framework were recently enhanced, with the new General Data Protection Regulation ("GDPR") coming into effect in May 2018. The EU considers the protection of personal data a fundamental right. The data protections afforded by the EU, however, also have significant extraterritorial implications, especially for technology and social media companies wishing to transfer user data overseas. This part examines the foundations of the EU’s data protection framework and its current state, as well as recent legal challenges brought against it. The discussion proceeds to examine the regulatory framework governing online political advertising in the U.S., before examining how that framework interacts with the European data protections in Part II.

i. Fundamental Rights

The EU possesses a comprehensive omnibus protection of the right to privacy.17 In the words of James Whitman, the European approach to privacy protection is “a form of protection of a right to respect and personal dignity.”18 This approach rests on the understanding that individuals should have the right to protect their public image – at its core, Whitman argues, this concerns the right of individuals to be “shielded against unwanted public exposure – to be spared embarrassment or humiliation.”19 In the context of online presence, it is thus in line with the European conception of privacy to enact strong protections for all online activity that might involve such public

18 Whitman, supra note 17, at 1161.
19 Id.
exposure. The European Charter of Fundamental Rights establishes the legal basis for a right to privacy. It became legally binding on EU Member States and Institutions after the Treaty of Lisbon came into force in 2009. Article 7 of the Charter establishes a fundamental right to respect of private life, and Article 8 the fundamental right to protection of personal data. The importance of protecting these rights has consistently been emphasized in European Union case law.

The U.S. approach to regulating privacy differs significantly from the European approach. In contrast to the EU’s omnibus protection approach, the U.S. has a collection of statutes and regulations that control privacy in specific areas and industries. According to Whitman, the American approach to privacy is “oriented toward values of liberty, and especially liberty against state.” Thus, the American approach to privacy protection limits government involvement. This partly explains why, for example, the FEC has taken a restrained approach to regulating online activity.

ii. Data Protection Directive

To protect this right to data privacy, the European Union enacted Directive 95/46/EC, commonly known as the “Data Protection Directive,” in October 1995. The Directive was designed to “give substance to the principles of the right to privacy already contained in [the] Convention, and to expand them.” It applied to all European Union member states, as well as three non-member state countries that are a part of the European Economic Area. Under the Directive, personal data could only be transferred to third countries (i.e. countries that are not members of the Directive, such as the United States) if those states guaranteed an adequate level of protection or took other special precautions. The adequacy of protection was determined by taking into consideration the particular circumstances of the data transfer. According to the Directive, “particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in

---

22 Charter of Rights, supra note 20, arts. 7–8.
24 Safari, supra note 17, at 809 n.1; see also Whitman, supra note 17, at 1156.
25 Whitman, supra note 17, at 1156.
26 See Edward R. Alo, Comment, EU Privacy Protection: A Step towards Global Privacy, 22 MICH. ST. INT’L L. REV. 1095, 1101 (2014) (noting that the U.S. courts have found the Bill of Rights to protect the privacy of individuals against government interference in specific instances).
27 See discussion infra Part I B(i).
the third country in question and the professional rules and security measures which are complied with in that country."31

iii. US-EU Safe Harbor Agreement

In light of the restrictions on transfers to third countries, the U.S. and EU negotiated a Safe Harbor Agreement to allow data transfers from Europe to the U.S.32 The U.S. Department of Commerce issued the Safe Harbor Privacy Principles in 2000.33 Shortly thereafter, the European Commission recognized the Principles by issuing Commission Decision 2000/520/EC.34 The Safe Harbor Agreement was a mechanism that ensured businesses and other entities could transfer data legally across the Atlantic. One of its key features was a self-certification process, which allowed American companies to self-certify their compliance with seven principles and related requirements to meet the data privacy adequacy standards of the EU.35 The self-certification process involved several requirements, such as making the organization’s privacy policy publicly available, naming a contact office responsible for responding to complaints, naming the statutory body with jurisdiction to hear claims against the organization, and naming any designated verification procedures (e.g. in-house or third-party).36

iv. The General Data Protection Regulation

The European Union’s data protection framework has recently undergone major changes. In April 2016, the European Union enacted the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018.37 The Regulation replaces the Data Protection Directive, and unlike the Directive, is directly applicable and thus does not require implementation measures from member states to be legally binding. Consequently, member state laws in this respect are set to be harmonized, i.e. largely brought into conformity across the member states. First proposed by the European Commission in 2012, this new framework has been enacted in response to technological developments in data sharing and collecting since the implementation of the Data Protection Directive.38 Important changes in the GDPR include providing people with “easier access to the data companies hold about them,” increased fines,
and a responsibility for organizations to “obtain the consent of people they collect information about.”\textsuperscript{39}

Under the GDPR, the European Commission has authority to impose significant financial penalties for non-compliant entities: \textsuperscript{40} up to 4% of the company’s global revenue or 20 million Euro, whichever is higher.\textsuperscript{41} The new regulation expands the existing data protection framework. Yet, in relation to data transfers to third countries, the G3DPR bases its framework largely on the earlier Data Protection Directive. Article 45 of the GDPR provides for transfers on the basis of an adequacy decision by the Commission\textsuperscript{42} (such as the provision enabling the creation of the EU-U.S. Privacy Shield). Moreover, Article 46 provides several additional grounds for data transfers, but all are subject to the data controller or data processor providing that appropriate safeguards are in place for the protection of that data.\textsuperscript{43}

v. ECJ Case Law: Schrems v. Data Protection Commissioner

The Safe Harbor framework came to a halt in 2015, when the European Court of Justice (“ECJ”) deemed that it was invalid in Schrems v. Data Protection Commissioner. The case arose from a complaint brought by Maximillian Schrems, an Austrian data privacy advocate, against the Irish Data Protection Authority.\textsuperscript{44} The complaint concerned Facebook’s transfers of Schrem’s user data from its EU-based servers in Ireland to the company’s servers in the U.S. In deciding the case, the Court considered the exceptions in the Safe Harbor Framework contained in Annex I to the Commission Decision 2000/520, which limited the Safe Harbor Principles “to the extent necessary to meet national security, public interest, or law enforcement requirements.”\textsuperscript{45} It found that as written, if there was a conflict between U.S. law and the Safe Harbor Principles, U.S. law would have primacy.\textsuperscript{46} Similarly, where national security, public interest, or law enforcement requirements conflicted with the Safe Harbor Principles, U.S. companies were “bound to disregard [the Safe Harbor] principles without limitation.”\textsuperscript{47}

Consequently, the Court held that the Safe Harbor Framework was invalid under EU law. It concluded that the Safe Harbor framework “enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States.”\textsuperscript{48} Notably, the


\textsuperscript{40} Sarah Gordon, \textit{Businesses failing to prepare for EU rules on data protection}, FIN. TIMES, (June 18, 2017), https://www.ft.com/content/28f4ef8-51bf-11e7-a1f2-db19572361bb [https://perma.cc/HU7E-63WM].

\textsuperscript{41} Council Regulation, \textit{supra} note 37, at art. 83(5) [hereinafter GDPR].

\textsuperscript{42} \textit{Id.} at art. 45.

\textsuperscript{43} \textit{Id.} at art. 46.

\textsuperscript{44} Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 EUR-Lex CLEX LEXIS 650.

\textsuperscript{45} \textit{Id.} at ¶ 84.

\textsuperscript{46} \textit{Id.} at ¶ 85.

\textsuperscript{47} \textit{Id.} at ¶ 86.

\textsuperscript{48} \textit{Id.} at ¶ 87.
Court was concerned with how the Safe Harbor framework provided public authorities generalized access to the content of electronic communications, finding that this violated the fundamental right to respect for private life.\(^{49}\) Furthermore, the Court determined that the Safe Harbor framework did not provide adequate legal remedies to European Union persons whose data might have been compromised, thus violating the fundamental right to effective judicial protection.\(^{50}\)

vi. EU-US Privacy Shield

After the invalidation of the Safe Harbor framework, EU and American officials negotiated a new data transfer agreement – the EU-US Privacy Shield. One of the objectives of this framework was to remedy the problems identified by the ECJ in the Schrems decision. On February 2, 2016, EU and U.S. officials announced their agreement on the new Privacy Shield.\(^{51}\) The agreement required approval by the European Commission, and on July 12, 2016, the European Commission announced its Implementing Decision, stating that the Privacy Shield provided adequate protection to allow data transfers between the EU and the U.S. in light of the Data Protection Directive.\(^{52}\)

The Privacy Shield imposes greater obligations on companies than the Safe Harbor Framework.\(^{53}\) The Principles required by the Privacy Shield follow a structure generally similar to the Safe Harbor, but several Principles have been expanded.\(^{54}\) Both sets of Principles lay out the requirements for conducting transatlantic data transfers in accordance with the EU data protection regime. Just like the Safe Harbor Principles, the Privacy Shield Principles include the Principles of notice, choice, accountability for onward transfers to third parties, security, data integrity, and access.\(^{55}\) The seventh Principle, not covering “recourse, enforcement, and liability”\(^ {56}\) affords more extensive remedies for EU citizens who believe that a U.S. company has violated their data protection rights, thus addressing the problem of inadequate access to remedies in the Safe Harbor framework. In 2016, President Obama also signed the U.S. Judicial Redress Act, which “will give EU citizens access to U.S. courts to enforce privacy rights in relation to personal data transferred to the United States for law enforcement purposes.”\(^ {57}\) The Privacy Shield includes 16 further supplemental
principles that discuss topics such as sensitive data, secondary liability, obligatory contracts for onward transfer of data to third parties, and access requests by public authorities. Finally, it provides an annual review mechanism where EU and U.S. officials will monitor compliance with the Privacy Shield.

vii. Challenges to Privacy Shield and Third Country Data Transfers

The Privacy Shield came under attack shortly after the European Commission authorized it. The European Parliament passed a resolution in April 2017 expressing significant concerns about the adequacy of the protections afforded by the Privacy Shield, particularly on the possibility of transferred data being vulnerable to mass surveillance by the U.S. government. Similarly, the Article 29 Working Party (“WP29”), an independent European advisory body on data protection and privacy, called for a reexamination of the Privacy Shield in November 2017. The report issued by the WP29 in November 2017 highlighted important unresolved issues concerning the Privacy Shield, such as “the lack of guidance and clear information on […] onward transfers and on the rights and available recourse and remedies for data subjects.”

Most significantly, the report outlined serious concerns with the access provided to U.S. public authorities for data transferred to the U.S., and called for greater transparency on the use of the U.S. government’s surveillance powers. The WP29 called for “further evidence or legally binding commitments to substantiate the assertion by the U.S. authorities that the collection of data under section 702 of the [Foreign Intelligence Surveillance Act (“FISA”)] is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program.” FISA section 702 is a statutory provision that allows the U.S. authorities to collect emails and other communications of non-US citizens abroad from American firms (such as Google, Facebook, and Twitter) without a warrant. Despite these concerns, President Trump

---

58 Id.
63 Id. at 3.
signed a reauthorization of FISA section 702 into law on January 19, 2018,\textsuperscript{66} signaling little change in U.S. policy towards FISA. The WP29 called for the U.S to remedy the highlighted issues before May 25, 2018, the date the new General Data Protection Regulation is set to take effect and noted that if changes were not made in time, the members of WP29 would take legal action to challenge the Privacy Shield Adequacy Decision in EU member state national courts.\textsuperscript{67} However, WP29 did not bring a legal action and neither has its successor, the EDPB. Instead, it has opted to meet with US representatives at its second plenary meeting, and noted that the aforementioned issues would “remain on the top of the agenda for the Second Annual Review [of the Privacy Shield]” scheduled for October 2018.\textsuperscript{68} Meanwhile, in June 2018, the European Parliament adopted a resolution calling for the European Commission to suspend the Privacy Shield until the U.S. fully complies with its terms.\textsuperscript{69}

The Irish Data Protection Commissioner (“DPC”) and Maximilian Schrems filed a further legal challenge against the validity of the use of Standard Contractual Clauses (“SCS”) as the basis of third country data transfers in \textit{DPC v. Facebook}.\textsuperscript{70} With regard to data transfers, SCS include two sets of model contractual clauses that the European Commission has authorized as offering sufficient safeguards on data protection to allow the data to be transferred internationally.\textsuperscript{71} The case rose to the High Court in Dublin, which issued an order on October 3, 2017 finding that the DPC had presented “well-founded concerns” over the validity of past European Commission decisions approving the use of SCS as a basis for third-country transfers\textsuperscript{72} and the DPC also had raised “well-founded concerns that there is an absence of an effective remedy in U.S. law […] for an EU citizen whose data are transferred to the U.S. where they may be at risk of being accessed and processed by U.S. state agencies for national security purposes.”\textsuperscript{73} The Court thus found that there was a basis to refer the case for preliminary reference to the ECJ.\textsuperscript{74} The Irish High Court formally referred the case to

\begin{itemize}
  \item Google and AT&T, the emails and other communications of foreigners abroad — even when they are talking to Americans.”).
  \item \textsuperscript{69} EUR. PARL. DOC. (COM 2645) ¶ 35 (2018).
  \item \textsuperscript{70} See \textit{Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems}, 2017 I.E.H.C 545 (H.Ct.) (Ir.).
  \item \textsuperscript{72} \textit{Id.} at 3.
  \item \textsuperscript{73} \textit{Id.} at 4.
\end{itemize}
the ECJ in April, 2018. No date has been set for the preliminary reference procedure as of October 2018.

In summary, the most important legal bases for data transfers from the EU to the U.S. under the GDPR face a considerably uncertain future. The developments described above present serious challenges for companies seeking to transfer personal data to the U.S. on an ongoing basis, including for the purpose of regulating the purchase of political online ads by foreigners.

B. U.S. Regulation of Online Political Advertising

To comprehensively examine the challenges to the regulation of foreign political advertising, and how these challenges interacts with the European data protection framework, we must first examine the U.S. regulatory landscape covering online political advertising.

i. FEC Regulation of Online Advertising

The Federal Election Commission (“FEC”) has taken a restrained approach to regulating online activity. The FEC has stated that a “disclaimer must appear on any electioneering communication [...] and on any public communication by any person that expressly advocates the election or defeat of a clearly identified candidate or solicits funds in connection with a federal election.” These disclaimer rules apply clearly to traditional political advertising and electioneering communications. When a political action committee spends money on an election-related communication, it is required to provide a disclaimer stating the source of the funding, such as those that follow television campaign ads.

Unlike these traditional media, online political advertising has been largely exempt from these rules. The FEC promulgated a coordination standard after the passage of the Bipartisan Campaign Reform Act in 2002, in which it held that internet communications were excluded from the definition of “public communications.” However, a district court struck down this wholesale exclusion in *Shays v. FEC*, holding that it was unreasonable and in conflict with the Act. In response to this decision, the FEC promulgated a rule regulating “only those internet communications placed for a fee on the website of another.” In 2006 it also promulgated additional

---

75 The Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems, 2016 No. 4809 P. (H. Ct.) (Ir.).
76 See Internet Communications, 71 Fed. Reg. 18,589, (Apr. 12, 2006) (stating that “the Internet warrants a restrained regulatory approach.”).
78 See id.
79 Typically, these follow the advertisement and are phrased in terms such as “This ad was paid for by X candidate for Congress.”
82 Id. at 1723.
83 Id. at 1724.
rules that aimed to protect internet communications other than paid advertisements
from regulation. By doing so, in effect, the FEC left a loophole in the regulatory
framework of political activity on the internet. Today, internet communications
that are disseminated for free are not considered “public communications” and are thus
automatically uncoordinated. As a result, such communications may be made with the
candidate’s direct involvement, can be funded with corporate or union money, and
may exceed the contribution ceiling.”Most online platforms are therefore
unregulated by federal election law, as they do not fall under the BCRA definitions of
“public communication” or “electioneering communications.”

While many technology platforms are considered websites available to the public
and would thus generally be subject to disclaimer rules, certain companies, such as
Facebook, have successfully lobbied for and received an exemption from these rules. In
certain situations, the FEC exempts advertisements from disclaimers when they are
practically inconvenient to provide, such as on small items like bumper stickers, pens,
and campaign buttons. Google and Facebook successfully argued in 2010 and 2011,
respectively, using the small items exception, that online ads were too small,
character-limited, and otherwise unsuitable to require disclaimers. They have since
been exempted from requiring disclaimers, despite significant advances in the
technology features on their online advertisements.

That said, the FEC has recently indicated that it may be reversing course on the
small items exemption it has applied to Facebook since 2011. The agency issued an
advisory opinion in December 2017 to the Take Back Action Fund, a conservative
political group, saying that it must include a disclaimer on all image and video
advertising published on Facebook advocating for the election or defeat of clearly
identified federal candidates. The advisory opinion has been interpreted as an early
sign that the FEC is reassessing the disclaimer rules applied to online political

---

84 Id. at 1724.
85 Id. at 1726–27.
86 Laura C. Bartelt, Citizens United and Political Advertisements: Corporations ’ Lucky Loophole to
the Unregulated Internet, 37 J. CORP. L. 415, 420 (2012).
87 FEC, supra note 77, (“Political committees must include a disclaimer on (1) all “public
communications” (defined below), (2) bulk electronic email (defined as electronic mail with more than 500
substantially similar communications) and (3) web sites available to the general public, regardless of
whether the communication expressly advocates the election or defeat of a clearly identified candidate, or
solicits funds in connection with a federal election (i.e., contributions for a federal candidate or federal
political committee”).)
88 See Frier & Allison, supra note 80.
89 FEC, supra note 77, (“Disclaimer Placement is Inconvenient In situations where a disclaimer notice
cannot be conveniently printed, the notice is not required. This provision affects items such as pens, bumper
stickers, campaign pins, campaign buttons and similar small items. Further, a disclaimer notice is not
required for communications using skywriting, clothing, water towers or other forms of advertisement
where it would be impracticable to display the disclaimer notice.”).
90 Kenneth P. Doyle, FEC Votes to Explore Disclosure Rules for Online Ads, BNA.COM, (Sept. 14,
Oct. 4, 2018) (“Advisory Opinions are official [FEC] responses to questions about how the federal campaign
finance law applies to specific factual, situations.”).
92 Letter from the Federal Election Commission to the Take Bake Action Fund (Dec. 15, 2017),
An important distinction in disclaimer rules is that the FEC does not impose the same disclosure requirements on so-called “issue ads”, i.e. political advertisements that do not specifically advocate for or against the election of a candidate for office. Therefore, a significant amount of political advertising on major online platforms is currently unregulated. Finally, the FEC in October filed an Advance Notice of Proposed Rule Making on internet communication disclaimers. For further discussion on these changes, see Part II of this note.

ii. Federal Communications Commission Transparency Requirements

In addition to the FEC disclosure requirements, political advertising transmitted via cable and satellite television and radio is subject to transparency requirements imposed by the Federal Communications Commission (“FCC”). After the passage of the Bipartisan Campaign Reform Act (“BCRA”) of 2002, Congress amended the Federal Communications Act of 1934 to require that “information regarding any request to purchase advertising time made on behalf of a legally qualified candidate for public office” must be placed in a political file maintained by the provider. The political file is a record maintained by any broadcast service licensee of all request for broadcast time made by or on behalf of a candidate for public office. The BCRA also expanded these political file requirements to include any advertisements discussing any “political matter of national importance.” As of 2016, those records have been posted publicly online. These requirements, however, do not apply to political advertisements transmitted online.

iii. Political Activity by Foreign Nationals

Political activity by foreign nationals is regulated chiefly by the Federal Election Campaign Act (“FECA”). FECA prohibits foreign nationals from directly or indirectly making political contributions or donations of money or other things of value in connection with any federal, state, or local election. Although FECA does not restrict foreign nationals from speaking out and advocating for positions on political issues, it prevents foreign nationals from “provid[ing] money for candidates or political parties or spend[ing] money in order to expressly advocate for or against the election of a candidate.” Moreover, FEC regulations concerning political activity

---

96 Expansion of Online Public Obligations to Cable and Satellite TV Operators and Broadcast and Satellite Radio Licensees ¶ 8 (FCC Rcd. 16-4).
97 47 C.F.R. § 73.1943.
98 FCC, supra note 96, ¶ 8.
99 Id. at ¶ 1.
100 Id.
by foreign nationals “prohibit foreign nationals from directing, dictating, controlling, or directly or indirectly participating in the decision-making process of any person [...] with regard to any election-related activities.”103 It follows that under the current framework, foreign nationals may not directly contribute to U.S. election campaigns. Thus, foreign nationals are not permitted to purchase online ads advocating for or against a specific candidate, but they are not restricted from purchasing ads taking positions on specific political issues.

PART II

Proposed Legislation to Address Foreign Interference in U.S. Elections

American legislators and commentators have proposed several regulatory solutions to address the problems of foreign interference in U.S. elections through online political advertising. Those proposals include the Honest Ads Act, an act introduced in Congress in October 2017,104 and the We the People Democracy Reform Act introduced in September 2017.105 The FEC also issued an Advance Notice of Proposed Rulemaking106 which, through its comment process, has attracted policy proposals from members of both houses of Congress, as well as industry and consumer groups.

A. U.S. Policy Proposals to Address Foreign Political Advertising

i. Honest Ads Act

A bipartisan group of Senators introduced the Honest Ads Act in Congress on October 19, 2017.107 The bill aims to overhaul the way online political advertising is regulated, and to address the problem of foreign interference in U.S. election through online political advertising. The new Act would require online technology companies such as Google and Facebook to retain copies of political ads and make them publicly available. The bill would also require these companies to “release information on who those ads were targeted to, as well as information on the buyer and the rates charged for the ads.”108 The companies would further be “required to keep and release data on anyone spending more than $500 on political ads in a year.”109 Applying a requirement similar to the FCC political file requirements currently applied to television and radio stations, “platforms with more than one million users

106 Internet Communications Disclaimers, supra note 95.
107 Supra note 105.
would also be required to maintain public records of political ad buys over $10,000.**

**ii. We the People Democracy Reform Act**

A group of Democratic Senators and Members of the House of Representatives introduced the We the People Democracy Reform Act of 2017 in September 2017. The proposed legislation does not address foreign political advertising as directly as the Honest Ads Act, but would have an impact on online political advertising more generally. The bill contains a comprehensive election law reform proposal, one aspect of which is increased transparency for campaign ads run on the internet. It calls for the expansion of political advertising disclosure requirements to audio and video communications transmitted through the internet and email. This provision would significantly increase the disclosure requirements for all online video and audio content made by anyone advocating for or against the election of a candidate for office. These proposed changes, however, do not cover so-called issue ads.

**iii. FEC Proposed Rulemaking on Internet Communication Disclaimers**

In October, 2017, the FEC filed an Advance Notice of Proposed Rulemaking (NPRM) where it requested “comments on whether to begin a rulemaking to revise its regulations concerning disclaimers on certain Internet communications, and, if so, what changes should be made to those rules.” The NPRM seeks, for example, comments on possible technological modifications to the current disclaimer requirements, how “small” internet advertisements (subject to an exemption from disclaimer rules) should be defined and whether providing a link to a page containing a disclaimer could work, as well as proposals that might minimize the need for revisions to the rules to new or emerging technology.

During the comment period, the FEC received a record number of over 150,000 comments, of which reportedly 147,320 (over 98%) supported the launch of the proposed rulemaking, 2,262 opposed the rulemaking and 190 were neutral. The FEC comments include a variety of policy proposals on the issue of internet disclosures. Proposals filed by a group of Senators and by a group of Members of Congress are indicative of two alternative regulatory approaches. A comment filed by 15

---


112 See We the People Democracy Reform Act, supra note 105 (Stand by Your Ad. Calls for the amendment of Section 318(d)(1) of the Federal Election Campaign Act of 1971 so as to apply to audio and video portions of communications transmitted through internet or electronic mail the same campaign advertising disclosure requirements that apply to communications transmitted through radio and television).

113 Id. at 63,569.

Democratic senators led by Senators Warner, Klobuchar, and McCaskill suggested that the FEC should work to “close loopholes [in the existing disclaimer rules] that have allowed foreign adversaries to sow discord and misinform the American electorate.” Specifically, the comment calls for the FEC to “take immediate and decisive action to ensure parity between ads seen on the internet and those on television and radio.”

The alternative proposal filed by 18 Members of Congress led by Congressmen Sarbanes and Conyers suggested a more drastic change, claiming that “the issuance of new guidelines for internet communication disclaimers is not enough.” Instead, this proposal called for a “separate, broader rulemaking that address head-on the topic of illicit foreign activity in U.S. elections.” The Sarbanes comment does not provide specific steps for how to address the problem of foreign political advertising.

iv. Industry Self-Regulation

An alternative solution to online political advertising is to leave the industry to address these issues on its own, i.e. to rely on so-called industry “self-regulation.”

In 2017, Facebook, Twitter, and Google announced several measures addressing some of the problems of foreign interference in American elections. For instance, Facebook CEO Mark Zuckerberg announced in September that Facebook was taking steps to “protect election integrity and make sure that Facebook is a force for good in democracy.” He outlined nine steps Facebook would take to further this effort, including working with Congress to investigate reported Russian interference and cooperating with election commissioners around the world. Most significantly, in September 2017, Facebook announced that political advertisers on its platform would target the political ads.

---


117 Id.


119 Id.


need to “disclose which page paid for an ad” and allow users to “visit an advertiser’s page and see the ads they’re currently running on any audience on Facebook.”123 In January 2018, Facebook announced these features would go live in the United States by summer 2018.124 As part of this feature, political advertisers are required to verify their identity, including “both their entity and location.”125 Now political advertisements include “Paid for by” -disclaimers, and users are able to click on the disclaimers to see details about the advertiser.126 Finally, Facebook voluntarily turned over to Congress 3,000 ads issued by Russian-linked accounts in connection with the 2006 presidential election in October, 2017.127

Google has also announced that it would be “working closely with lawmakers and industry to improve transparency, accountability, and disclosures around election advertising.”128 In addition, in 2018, it announced that it would “release a transparency report for election ads, which will share data about who is buying election-related ads on our platforms and how much money is being spent.”129 The ad transparency report was launched in August 2018.130 The company also introduced a public database of “election ads purchased on AdWords and YouTube” containing information about who bought each ad.131 They include in-ad disclosures identifying the names of advertisers running election-related campaigns on its platforms, as well as instate a verification program requiring that advertisers “proactively identify who they are and where they are based before running any election-related ads.”132

Twitter reported in October 2017 that it would create an “Advertising Transparency Center” that will offer “visibility into who is advertising on twitter [and] details behind those ads.”133 The Ads Transparency Center went live in June 2018.134 Twitter noted specifically that “there is currently no clear industry definition for issue-based ads,” but that it would work with peer companies, policy makers, and ad partners

123 Id.
126 Zuckerberg, supra note 125.
129 Id.
132 Id.
to clearly define them and integrate them into the new approach. Other platforms that have initiated political advertising transparency initiatives include Snapchat, which requires political advertisements to "clearly identify who paid for the communication and whether or not the ad was authorized by a candidate and/or organization." 

Social media and internet platforms face conflicting interests concerning the disclosure of political advertisements. On one hand, these platforms thrive on public trust. Encouraging users to trust and engage with them is an essential feature of their business models – it enables them to retain and grow user engagement. Maintaining this user trust is particularly important, considering the vast amounts of sensitive personal user data social media platforms today are privy to and possess. At the same time, a favorable public perception and trust in these platforms may reduce calls for increased regulation and surveillance of these platforms, reducing the cost and complexity of regulatory compliance.

On the other hand, social media platforms also have commercial incentives to grow the sphere of political advertising. Political advertising is a significant and growing industry, and an important source of revenue for large social media platforms. For example, the 2016 United States local, state, and federal election cycle saw a total of $1.415 billion spent on online advertising, a 789% increase in spending from 2012. So, while industry participants in this sector have an incentive to police and regulate fraudulent and disruptive political spending, their interest in doing so may be tempered partly by other commercial considerations. Indeed, in the past these platforms have consistently advocated to be exempt from FEC political disclosure requirements. For example, Facebook argued in 2011 that stricter FEC regulations would stand in the way of innovation.

PART III

European Data Protection and US Legislative Efforts

This section considers the US legislative proposals described above in light of the European Data Protection Framework, examining the challenges that European Data Protection rules may pose for the proposed legislation.

A. Legislative Proposals in light of European Data Protection Framework

European data protection rules present several possible limitations on the effectiveness of these proposed regulatory solutions. In addressing these questions, it is most helpful to center the discussion on analyzing the policy proposals under the

135 Id.


General Data Protection Regulation ("GDPR" or "Regulation"). These became binding in May 2018, replacing the prior data protection framework. The most significant issues that the GDPR presents for the regulation of foreign political advertising stem from a provision in the GDPR limiting the transfer of personal data to third countries.

i. Territorial Reach of the GDPR

The territorial scope of the GDPR is expansive. Article 3(1) of the Regulation establishes that the Regulation applies to the processing\(^\text{139}\) of "personal data in the context of activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."\(^\text{140}\) Thus, any corporate entity established in the EU would be covered by the Regulation, even for activities conducted outside of the EU. Additionally, recent ECJ decisions such as the Google Spain\(^\text{141}\) case and Schrems case (as discussed in Part I above) have established that the ECJ interprets "establishment" expansively for the purposes of the Data Protection Directive. This is likely to carry over to the GDPR once it takes effect.\(^\text{142}\)

The territorial reach of the GDPR also extends to the processing of all personal data of any natural person physically present in the EU. This provision concerning data processing applies regardless of citizenship or residency status, thus including individuals who are only passing through the EU, such as tourists.\(^\text{143}\) It also applies to processing by any company that processes data in connection with the offering of goods or services (whether or not for payment) to such natural persons in the EU and “for the monitoring of their behavior as far as their behavior takes place within the Union.”\(^\text{144}\) This provision thus extends the GDPR’s reach to any company not established in the EU that offers goods or services in the EU or monitors user behavior in the EU. Article 4(1) of the GDPR defines personal data expansively as applying to any information relating to “an identified or identifiable natural person.”\(^\text{145}\) Thus, any information, such as the name, online identifier, or location data that could be used to identify a natural person purchasing political advertisements, would fall under the

---

\(^{139}\) GDPR, \textit{supra} note 42, art. 4(2) (defines "processing" as follows: "‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.")

\(^{140}\) Id.

\(^{141}\) In this case, the ECJ established the so-called “right to be forgotten”, in other words, an EU citizen’s right to request commercial search firms to remove links to private information in certain situations. Case C-131/12, Google Spain v. Agencia Espanola de Proteccion de Datos, 2014 ECR 317.

\(^{142}\) Shakila Bu-Pasha, \textit{Cross-Border Issues Under EU Data Protection Law with Regards to Personal Data Protection}, 26 \textit{INFO. \\& COMM. TECH. L.} 213, 217 (2017) ("By finding Google Spain as an ‘establishment’ of Google Inc. under Article 4(1)(a) and within the meaning of Recital 19 of the DPD, the CJEU found them ‘inextricably linked’ and thereby permitted interpretation of the DPD with extraterritorial jurisdiction.").

\(^{143}\) GDPR, \textit{supra} note 42, art. 3(2).

\(^{144}\) Id.

\(^{145}\) Id. art. 4(1) (defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identified such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”).
definition. Therefore, to the extent any social media platform sells political advertisements to users located in the EU, they are subject to the GDPR.

ii. Third Country Data Transfers under the GDPR

A significant challenge for potential policy solutions to foreign political advertising in U.S. elections are the restrictions on the transfer of any personal data to third countries imposed by the GDPR. As discussed in Part I, the GDPR only allows transfers of personal data to third countries (i.e. countries not party to the GDPR, such as the U.S.) if the EU deems those countries to have adequate levels of data protection in place. Thus, social media platforms seeking to transfer and provide personal data about the purchasers of U.S. political ads located in Europe have two options: (1) obtain an adequacy decision from the European Commission under Article 45 of the GDPR\textsuperscript{146}, such as under the Privacy Act, or (2) use approved alternative procedures subject to Appropriate Safeguards under Article 46 of the GDPR, such as SCS or Binding Corporate Rules ("BCR").

As discussed in Part I, these legal bases have come under challenge from a number of parties. The Article 29 Working Party ("WP29") expressed severe concerns about the adequacy of the Privacy Shield in light of U.S. mass surveillance programs, in particular the FISA section 702 provision. The WP29 asked U.S. regulators to ensure that the FISA section 702 provision is not used indiscriminately and on a generalized basis.\textsuperscript{147} FISA section 702 allows authorities to collect data about foreign citizens from companies such as large social media platforms. Given that President Trump reauthorized the FISA section 702 provision into law without significant changes, it is unlikely that the U.S. government will be able to satisfactorily address the WP29’s concerns. The adequacy of the Privacy Shield is therefore likely to come under challenge.\textsuperscript{148} A central basis for the ECJ’s ruling invalidating the Safe Harbor Agreement in Schrems v. Irish Data Protection Commissioner\textsuperscript{149} was the finding that “legislation permitting the [U.S.] public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.”\textsuperscript{150} So, the ECJ could invalidate any adequacy decision that did not address the FISA section 702 concern, presenting a significant challenge for the future of Transatlantic data transfers.

The GDPR also permits transfers of personal data to third countries when those transfers are based on Commission-approved SCS. However, SCS’ adequacy is under challenge in DPC v. Facebook (also known as “Schrems 2.0”), a case seeking to invalidate this basis for data transfers. The Irish High Court examined the existing U.S. mass surveillance regime and found that there were well-founded concerns about

\textsuperscript{146} Id. art. 45.
\textsuperscript{147} WP29 Report, supra note 62, at 3.
\textsuperscript{149} Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, 2015 EUR-Lex CLEX LEXIS 650.
\textsuperscript{150} Id. at ¶ 94.
the sufficiency of remedies (as required by Article 47 of the Charter of Fundamental Rights) for EU data subjects whose data is at risk of being accessed by U.S. regulators, in violation of their right to privacy and data protection. Significantly, it found that there were well-founded concerns that SCS do not address the lack of required remedies available.151 This decision does not invalidate the use of SCS for now, but it highlights many of the same concerns that led the ECJ to invalidate the Safe Harbor Framework in Schrems v. DPC.152 The ECJ’s ruling on this matter could thus uproot one of the primary legal bases for transferring user data to the U.S. by challenging the adequacy of SCS.

iii. GDPR Derogations for Specific Purposes

It may be possible to avert the problems associated with the Privacy Shield and Contractual Clauses temporarily by conducting third country transfers in reliance on Derogations under Article 49 of the GDPR. As discussed in Part I, the GDPR contains derogations from the general prohibition on transfers of personal data outside the EU, two of which are most relevant here. The first is the derogation in Article 49(1)(a), for transfers which the “data subject has explicitly consented to […] after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.” This derogation, however, does not apply to activities carried out by public authorities in the exercise of their public powers (and could thus only apply to industry self-regulation measures.)153

The second is the derogation in Article 49(1)(d) for transfers that are “necessary for important reasons of public interest.”154 When relying on this derogation, the transfers may not be repetitive, must “concern[] only a limited number of data subjects”, and must be “necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject.”155 This significantly limits the ability of Social Media Platforms to use this Article as a basis for routinely transferring information about the identity of foreign political ad purchasers to the United States. Moreover, Article 49(4) further clarifies that this “public interest” which justifies the transfer for a public interest derogation must be “recognised in Union law or in the law of the Member State to which the controller is subject.”156 The GDPR does not specify whether the integrity of U.S. or other foreign elections would qualify as a public interest recognized in Union or Member State law.

151 See Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems, 2017 I.E.H.C 545 (H.Ct.) (Ir.).
152 See, e.g., Schrems v. Data Protection Commissioner, supra note 149, at ¶ 95 (emphasizing the necessity of a right to a legal remedy).
153 GDPR, supra note 42, art. 49(3).
154 Id. at art. 49(1)(d).
155 Id. at art. 49.
iv. Consent and Confidentiality of Personal Data

Assuming the third country transfers are approved, a further challenge for social media companies is determining whether they can make personal data public, as many of the policy proposals require. One way to achieve this is by requiring any political ad purchaser to consent to making their personal data public for some specific purpose (such as maintaining a public database for ad purchases), under Article 6(1)(a) of the GDPR. The GDPR lays out requirements for how this consent can be obtained, including requiring that the request for consent needs to “be presented in a manner which is clearly distinguishable […], in an intelligible and easily accessible form, using clear and plain language.”\footnote{GDPR, \textit{supra} note 42, art. 7(2).} The publication of this data could also be authorized by Article 6(1)(c), which allows processing “necessary for compliance with a legal obligation to which the controller is subject;” or Article 6(1)(e), which allows processing that is “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.” However, the basis of the processing in either of these provisions must be in European Union law or Member State law, i.e. there must be a justification for processing in EU or Member State law authorizing it.\footnote{Id. at art. 6(4)(e).} Article 6(4) provides a possible basis for processing and making public personal data when other bases are not available. There, the data controller must take into consideration factors such as the existence of appropriate safeguards (e.g. encryption or pseudonymization).\footnote{Id. at art. 6(4)(c).} In deciding whether to process personal data for a purpose other than that for which it was collected, the processor must take into account whether sensitive categories of information, such as information on the “political opinions, religious or philosophical beliefs” of a data subject are involved.\footnote{Colin Lecher, \textit{Senate Announces New Bill that Would Regulate Online Political Ads}, \textit{The Verge}, (Oct. 19, 2017), https://www.theverge.com/2017/10/19/16502946/facebook-twitter-russia-honest-ads-act [https://perma.cc/3GRN-P6TG].}

B. Online Political Advertising Policy Proposals and European Data Protection

i. Honest Ads Act and We the People Act

The two Congressional bills addressing the issue of online political advertising are also likely to be affected by European data protection rules. To the extent the Honest Ads Act calls for social media platforms to release information “on the buyer [of political ads] and the rates charged for the ads,” the ability of social media platforms to do so would be limited by the GDPR. As discussed above, personal data can only be transferred from the EU to the United States if there is an adequacy decision or some appropriate basis for transferring this data. This means that the platforms would need to first ensure they have a legal basis to make such third country transfers. The recent challenges to the Privacy Shield and SCS may jeopardize this. Moreover, the platforms might be able to rely on a derogation under Article 49. However, they will need to show either that they have obtained consent from the data

\footnote{157 GDPR, \textit{supra} note 42, art. 7(2).} \footnote{Id. at art. 6(3).} \footnote{Id. at art. 6(4)(e).} \footnote{Id. at art. 6(4)(c).} \footnote{Colin Lecher, \textit{Senate Announces New Bill that Would Regulate Online Political Ads}, \textit{The Verge}, (Oct. 19, 2017), https://www.theverge.com/2017/10/19/16502946/facebook-twitter-russia-honest-ads-act [https://perma.cc/3GRN-P6TG].}
subject, or that there is a public interest justification recognized by EU or member state law for performing the transfer.\textsuperscript{162}

Separate from the issue of third country data transfers, further issues remain regarding the data subject’s (i.e. the ad purchaser’s) consent. The platforms may need to obtain this consent to process their data, for the purpose of compiling and releasing the information of the purchasers of political ads.\textsuperscript{163} In the event that they do not have consent from the data subject, the platforms may need to pseudonimize the personal information. Beyond this, they may still face challenges to this type of nonconsensual release of sensitive personal information (relating to the political views of the data subject).\textsuperscript{164}

The We the People Act does not require the compilation of personal information about ad purchasers in the way the Honest Ads Act does. However, central to both bills is a requirement to include an increasing amount of disclosures on online political ads that identify the individual or entity paying for the ad.\textsuperscript{165} The disclosure of this information raises issues of data transfers to third countries, and requiring the consent of the data subject purchasing the ad for disclosing that information, as discussed above. If the platforms do not obtain consent, they face the same problems with the release of sensitive personal data.

ii. FEC Rulemaking

The proposed FEC rulemaking brings up issues very close to those common to both Congressional bills discussed in the paragraph above. Insofar as the FEC rulemaking would treat online political ads more like television or radio advertisements, they would also require a disclaimer about who purchased and paid for the ad in question.\textsuperscript{166} Thus, the same consent requirements apply. Similarly, the transfer of such personally identifiable data to the United States would implicate the issues discussed concerning third country data transfers.

iii. Industry Self-Regulation

The three largest social media platforms have all announced initiatives to require purchasers of political ads to disclose their identity. Per these announcements, these disclosures are to take the form of disclaimers attached to the ads themselves, or other functionalities implemented in their platforms.\textsuperscript{167} Industry self-regulation measures that require disclosure of who purchased political ads may run into largely the same GDPR issues discussed above in connection with FEC rulemaking and the Congressional bills. Explicit consent requirements can address the problem partly, but the publishing of sensitive data about political opinions could still attract EU

\begin{footnotes}
\footnotetext[162]{GDPR, supra note 42, art. 49(4); see also Albrecht Brief, supra note 157, (arguing that a “reason of public interest . . . can only be made by the courts of [the EU] or of the Member State in question, applying EU law under the supervisory jurisdiction of the [European Court of Justice].”).}

\footnotetext[163]{GDPR, supra note 42, art. 6(1)(a).}

\footnotetext[164]{Id. at art. 6(4)(e).}

\footnotetext[165]{We the People Act, supra note 105, at Sec. 1041(c); Honest Ads Act, supra note 104, at § 8(a)(1)(A).}

\footnotetext[166]{See supra Part II(A)(iii), and accompanying discussion.}

\footnotetext[167]{See Walker, supra note 128; Falck, supra note 133; Zuckerberg, supra note 122.}
\end{footnotes}
regulatory scrutiny. The biggest challenge for all competing approaches remains ensuring that data transfers can continue to the U.S. without disruption, i.e. that they are third country transfers authorized under the GDPR. However, to the extent that the ECJ’s and European Commission’s reservations about transfer of data to third countries is about U.S. government mass surveillance, industry self-regulation measures might stand a better chance of surviving ECJ or Commission review than measures that directly require the release of personal data about users to the U.S. government.

EU regulators have recently embraced self-regulation in one area of online activity: hate speech.168 The European Commission and four technology companies (Facebook, Microsoft, Twitter, and YouTube) signed a voluntary Code of Conduct on Countering Illegal Hate Speech Online (“Code”) on May 31, 2016. Under the Code, participating companies commit to review and remove flagged content that violates hate speech laws, within 24 hours.169 This approach arguably enhances efficiency as well as effective cross-border enforcement, as compared with a traditional regulatory approach.170 Yet, the Code is only one part of the EU’s framework for addressing hate speech, and was arrived at because of the difficulty in reconciling the varying degrees of free speech protection in different EU member states.171 American federal regulators attempting to address online political advertising may not need to reconcile a comparable variety of regulatory approaches in the United States as exists on the issue of hate speech between EU member states. Therefore, they might face fewer obstacles to finding a binding compromise and may be less inclined to accept a non-binding self-regulatory approach on this issue.

PART IV

Implications of European Data Protection Regulations and The Way Forward

The sections above consider how the European Data Protection Framework may impact specific U.S. political advertising legislative efforts. This section considers other, broader implications of European Data Protection Regulations, such as highlighting the privacy interests at stake and outlining certain limitations and potential challenges to regulatory efforts.

i. Privacy Interests at Stake

The regulation of online political advertising implicates the privacy interests of political ad purchasers in Europe. The process of purchasing political ads involves the collection of personal details, such as the identity and location of the purchaser, that could be linked to potentially sensitive information about an individual’s political opinions. The GDPR specifically designates political opinions as a special category of personal data, and generally prohibits its processing unless a particular exception

168 See generally, Hui Zhen Gan, Corporations: The Regulated or the Regulators? The Role of IT Companies in Tackling Online Hate Speech in the EU, 24 COLUM. J. EUR. L. 111 (2017).
169 Id. at 112–113.
170 Id. at 113.
171 Id. at 143.
applies.\textsuperscript{172} If U.S. regulations require social media companies to collect, transfer abroad, and publish information about European political ad purchasers, these companies may need to possess and publicize sensitive information about individuals’ political beliefs. The European data protection framework has designated privacy and data protection as fundamental rights\textsuperscript{173}, and this type of processing and disclosure could violate those rights.

Yet, it is debatable whether in the context of individuals buying ads about a foreign election, those individuals should have the same rights to privacy. If the individuals are acting out of an intent to sow discord in U.S. elections, for example,\textsuperscript{174} one can argue that there is a compelling countervailing public interest reason to disclose their identity. To address concerns such as these, the GDPR provides some avenues for balancing those interests, such as by allowing public interest derogations for data transfers.\textsuperscript{175} However, a further related complication might arise if there is an effort to regulate issue ads. For example, if a European purchaser buys an ad taking a position for or against abortions, would social media platforms be required to provide that information to U.S. regulators, if that ad could also be accessed by American users? This opens up potentially broader issues of protecting European users’ sensitive personal data, relative to those implicated in the purchase of advertisements to interfere with foreign elections.

ii. Third Country Transfers

The treatment of third country data transfers in the European data protection regime is the most consequential challenge posed by European regulations for regulating foreign online political advertising in the U.S. This is because foreign political interference virtually always involves an international data transfer, and it is in this area that the EU has significant regulatory power. The ECJ, Article 29 Working Party, European Parliament, and privacy activists, among others, have expressed significant concerns about the adequacy of data protections afforded to European data subjects in the United States.\textsuperscript{176} EU authorities have listed a number of problems, most significant of which are fears about U.S. Government mass surveillance programs, authorized in part under FISA section 702\textsuperscript{177}, as well as delays in appointing a data ombudsperson\textsuperscript{178} and members to the Privacy Civil Liberties Oversight Board\textsuperscript{179} as

\begin{flushleft}
\textsuperscript{172} GDPR, supra note 42, art. 9.
\textsuperscript{175} See supra Part II (B)(iii) and accompanying discussion.
\textsuperscript{176} See, e.g., Natasha Lomas, EU-US Privacy Shield Remains Precariously Placed, TECHCRUNCH (Apr. 6, 2017), https://techcrunch.com/2017/04/06/eu-us-privacy-shield-remains-precariously-placed (discussing some of the reasons the Privacy Shield received criticism).
\textsuperscript{177} See id. (discussing some of the European Commission’s concerns with the FISA 702 provision).
\textsuperscript{178} See id. (discussing the issues involving the appointment of an ombudsperson; a temporary acting ombudsperson was appointed in January 2019).
\textsuperscript{179} See Press Release, Eur. Comm’n, EU-U.S. Privacy Shield: First Review Shows It Works But Implementation Can Be Improved (Oct. 18, 2017) (IP/17/3966) (asking the U.S. government to ensure that the empty posts on the Privacy and Civil Liberties Board are filled as soon as possible).
\end{flushleft}
required by the Privacy Shield. As mentioned earlier, the current U.S. presidential administration signed an extension of FISA section 702 into law in January 2018.\(^\text{180}\) Thus, efforts to negotiate and ensure that a sufficient level of protection is in place to ensure the adequacy of the Privacy Shield as a basis for third country data transfers face heightened challenges.\(^\text{181}\) The success of the Privacy Shield may require a firm commitment from the U.S. government that FISA section 702 will not apply indiscriminately to European Union data subjects.\(^\text{182}\) Similarly, U.S. regulators need to ensure that remedies, such as those provided through the Presidential Policy Directive 28, are available to EU data subjects.\(^\text{183}\) Otherwise, the EU and U.S. regulators may need to find another way to determine that adequate data protections are in place to allow data transfers to continue.

As an alternative to the Privacy Shield and SCS, companies wishing to transfer user data to the United States could resort to Binding Corporate Rules (“BCRs”) as an adequacy basis under Article 47 of the GDPR.\(^\text{184}\) This process involves getting an approval from a data protection authority in one of the EU member states certifying that a company has sufficient internal legal protections in place to ensure adequate protection of subjects’ personal data.\(^\text{185}\) However, for large American social media companies, which may be subject to surveillance under FISA section 702 in the U.S., it is not clear that data protection authorities will be readily willing to certify the protections as adequate. In short, these BCRs may also be vulnerable to similar legal challenges as those brought challenging the adequacy of SCS.\(^\text{186}\)

The continuance of data transfers between Europe and the U.S. affects billions of dollars in business transactions annually.\(^\text{187}\) Therefore, the incentives to ensure the


\(^{181}\) Keane, supra note 148.

\(^{182}\) See, e.g., Mieke Eoyang & Gary Ashcroft, Why Electronic Surveillance Reform Is Necessary, Lawfare (Feb. 28, 2017), https://www.lawfareblog.com/why-electronic-surveillance-reform-necessary [https://perma.cc/3Q5X-6GYL] (arguing that FISA presents a challenge to the Privacy Shield and that the U.S. should reform the FISA process to ensure that continued transatlantic data flows.).


\(^{184}\) See, e.g., Joseph Wholley, III, Are You Ready for Binding Corporate Rules, IAAP (March 9, 2015), https://iapp.org/news/a/are-you-ready-for-binding-corporate-rules/ [https://perma.cc/6ZD3-7HSA] (for a discussion about the BCR mechanism.).

\(^{185}\) Id.


continued and stable transfer of personal data and to promote legal certainty for businesses extend well beyond the objective of effectively regulating online political advertising. This gives some cause for optimism that U.S. and EU regulators will guarantee a sustained basis for data transfers. However, these negotiations raise difficult choices between protecting U.S. national security and the integrity of its political institutions on the one hand, and addressing fundamental European concerns about the protection of privacy and personal data on the other.\footnote{188 See Deckelheim, supra note 53, at 290–91 (2016) (discussing the fundamental differences between U.S. and European authorities to privacy and national security).}

iii. Personal Data about Natural vs. Legal Persons

An important limitation to the scope of GDPR and European privacy regulations more generally is that they apply to the protection of personal data about \textit{natural persons, not legal persons}.\footnote{189 GDPR, supra note 41, art. 4(1).} User data about legal persons such as companies is thus not subject to GDPR protections. This type of data can be transferred relatively freely to the United States. Thus, any policy measure that seeks to disclose the name of e.g. a company or an organization purchasing an ad will not be limited by the GDPR or third country data transfer rules. Yet, the ability to obtain information about corporate or organizational entities but not to identify the individuals behind them will limit the utility of disclosing this type of information.

iv. Issue vs. Candidate-Specific Ads

A consequential distinction is that the policy framework in both congressional bills, the FEC disclosure comments, and much of the industry self-regulation measures only address ads specifically advocating for or against the election of a candidate.\footnote{190 See, e.g., supra discussion in Part III(B).} Ads advocating for or against specific \textit{issue} positions are not covered. Moreover, it is not unlawful for foreign citizens to spend money on these so-called issue ads in U.S. elections, as long as they are not coordinating these expenditures with candidates for political action committees.\footnote{191 Bluman \textit{v. FEC}, 800 F.Supp.2d 281, 290 (D.D.C. 2011), aff’d 565 U.S. 1104 (2012) (foreign national ban “does not restrain foreign nationals from speaking out about issues or spending money to advocate their views about issues.”); see 11 C.F.R. §110.20(c).} Hence, even if foreign expenditures on candidate-specific ads are successfully regulated, this leaves an important gap in the ability of foreign entities and citizens to influence U.S. politics and elections.

v. Impact on Third Country Nationals

While the GDPR is an EU regulation, its impact extends beyond offering protections to the nationals of EU countries. Specifically, the GDPR protects the personal data of all data subjects within the EU, whether they are temporary visitors or residents.\footnote{192 GDPR, supra note 41, art. 3(2).} Considering the recent concerns regarding Russian interference in U.S. elections, this has serious implications. Any Russian (or other third country) nationals who are present in the EU while making an ad purchase would be protected under the

\footnote{188 See Deckelheim, supra note 53, at 290–91 (2016) (discussing the fundamental differences between U.S. and European authorities to privacy and national security).}

\footnote{189 GDPR, supra note 41, art. 4(1).}

\footnote{190 See, e.g., supra discussion in Part III(B).}

\footnote{191 Bluman \textit{v. FEC}, 800 F.Supp.2d 281, 290 (D.D.C. 2011), aff’d 565 U.S. 1104 (2012) (foreign national ban “does not restrain foreign nationals from speaking out about issues or spending money to advocate their views about issues.”); see 11 C.F.R. §110.20(c).}

\footnote{192 GDPR, supra note 41, art. 3(2).}
This provides a potential avenue for individuals wishing to conceal their identity, thus obscuring the detection of foreign ad purchases.

vi. U.S. Criminal Enforcement

A further alternative channel for regulating foreign interference in U.S. elections is through criminal prosecution, as evidenced by the indictment involving Russian interference in the 2016 election,\textsuperscript{194} as well as the Justice Department charge against a Russian individual for interference before the 2018 midterm elections.\textsuperscript{195} Federal authorities can prosecute campaign finance violations under FECA when the violations satisfy certain criteria. To be a crime, a FECA violation must have been committed knowingly and willfully and cover an aggregate amount of at least $2,000 during a calendar year.\textsuperscript{196} This means that the Department of Justice could prosecute foreign spending on ads “expressly advocat[ing] for or against the election of a candidate”\textsuperscript{197} by individuals or entities who have spent more than $2,000 on such communications.\textsuperscript{198} Yet, U.S. authorities cannot bring criminal charges concerning most foreign-funded issue campaign ads, which are not prohibited by FECA.\textsuperscript{199} Neither can they generally criminally prosecute the purchase of ads by individuals or entities spending less than $2,000 annually. While there are other charges prosecutors can bring, these gaps in the statutory provisions significantly limit the possible regulation of foreign political spending through criminal enforcement.

A case before the U.S. Supreme Court\textsuperscript{200} has given light to possible challenges to the international sharing of personal information in the case of criminal enforcement. In\textit{ U.S. v. Microsoft},\textsuperscript{201} the Second Circuit held that the government cannot compel Internet Service Providers (“ISPs”) to provide data stored overseas, even pursuant to a warrant.\textsuperscript{202} In particular, the Court held that the warrant provisions of the Stored Communications Act (“SCA”) do not apply extraterritorially.\textsuperscript{203} This implies that the government must resort to the existing process for obtaining foreign-stored data pursuant to a warrant, namely, by relying on a Mutual Legal Assistance Treaty (“MLAT”), “which allow[s] signatory states to request one another’s assistance with ongoing criminal investigations, including issuance and execution of search warrants.”\textsuperscript{204} Article 48 of the GDPR permits third country data transfers when they are based on a decision of an administrative authority of that third country only if they

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{193} Id.
\item \textsuperscript{194} Indictment, United States v. Internet Research Agency (D.D.C. filed Feb. 16, 2017), https://www.justice.gov/file/1035477/download [https://perma.cc/7QNR-EHGG].
\item \textsuperscript{196} 52 U.S.C.A. § 30109(1)(A)(ii) (West 1971).
\item \textsuperscript{197} Bluman, 800 F.Supp.2d at 290.
\item \textsuperscript{198} 52 U.S.C. § 30121 (West 2012).
\item \textsuperscript{199} Bluman, 800 F.Supp.2d at 290.
\item \textsuperscript{200} United States v. Microsoft Corp. 138 S.Ct. 1186 (2018).
\item \textsuperscript{201} In re Microsoft Corp., 829 F.3d 197, 221 (2d Cir. 2016).
\item \textsuperscript{202} Id. at 222.
\item \textsuperscript{203} Id.
\item \textsuperscript{204} Id. at 221.
\end{itemize}
\end{footnotesize}
are based on an international agreement, such as a mutual legal assistance treaty ("MLAT").\footnote{GDPR, \emph{supra} note 41, art. 48.}

In an amicus brief submitted in the \textit{Microsoft} case, the European Commission argued that “Article 48 makes clear that a foreign court order does not, as such, make a transfer lawful under the GDPR.”\footnote{Brief for the European Union as Amicus Curiae, \emph{p. 14, United States v. Microsoft Corp.}, 138 U.S. 356 (2017).} Instead, the GDPR makes MLATs the preferred option for transfers.\footnote{\textit{Id.} at 14.} However, the transfer to a third country can only proceed if it additionally qualifies under Article 49,\footnote{\textit{Id.} at 14-5.} and derogations under Article 49 must be interpreted strictly.\footnote{\textit{Id.} at 16.} Several members of the European Parliament make similar arguments about the application of Article 49 in another amicus brief in the case.\footnote{Brief for Jan Philipp Albrecht et al. as Amici Curiae, \emph{United States v. Microsoft Corp.}, 138 U.S. 356 (2017).} They agree that Article 49 derogations must be construed narrowly.\footnote{\textit{Id.} at 17.} The amici go on to note that the exception for “important reasons of public interest” in 49(1)(c) cannot permit a transfer “simply because the data is requested by foreign law enforcement authorities.”\footnote{\_\_\_ at 16.} Further, the determination of what is a “reason of public interest” “can only be made by the courts of [the EU] or of the Member State in question, applying EU law under the supervisory jurisdiction of the [European Court of Justice].”\footnote{\textit{Id.}}

However, the bipartisan Clarifying Lawful Overseas Use of Data ("CLOUD") Act, introduced in the U.S. Senate in February 2018, could affect the impact of \textit{U.S. v. Microsoft}.\footnote{CLOUD Act, S. 2383, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/senate-bill/2383/text [https://perma.cc/4XYF-KAVW].} The bill would amend the SCA to apply to “all data that is in the possession, custody, or control of the provider, regardless of where the data is stored.”\footnote{Andrew K. Woods & Peter Swire, \textit{The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems}, \textsc{Lawfare} (Feb. 6, 2018), https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems [https://perma.cc/2SBB-A8WA].} In the event that a warrant compels ISPs to provide data in violation of the laws of the jurisdiction in which the data is located, the ISPs could move to quash the warrant.\footnote{Press Release, Senator Orrin Hatch (Feb. 5, 2018), https://www.hatch.senate.gov/public/index.cfm/2018/2/hatch-previews-cloud-act-legislation-to-solve-the-problem-of-cross-border-data-requests [https://perma.cc/WGE9-MN8T].} A court hearing the motion to quash would conduct a comity analysis to decide the motion.\footnote{\textit{Id.}} If passed, the bill may still receive push-back from EU regulators, as it would authorize data transfers outside of the MLAT procedure endorsed by Article 48 of the GDPR,\footnote{See Press Release, Open Technology Institute, OTI Opposes the CLOUD Act (Feb. 6, 2018), https://www.newamerica.org/oti/press-releases/oti-opposes-cloud-act/ [https://perma.cc/7PX8-6G4J].} allowing American, instead of European courts, to decide motions to quash. According to the Amicus Briefs filed by the
European Commission and several members of European Parliament, this would likely violate Article 48 of the GDPR.

vii. EU Enforcement

The GDPR contains significant sanctions provisions, allowing the European Commission to fine non-compliant companies up to 4% of their global annual turnover.\(^{219}\) European regulators also have additional tools for enforcing compliance. Namely, the European Commission has in recent years levied substantial fines against foreign technology companies in other areas, including antitrust fines against Google in the amount of $2.7 billion, and ordering Apple to pay $14.5 billion in back-taxes to Ireland, showing its readiness to impose harsh sanctions.\(^{220}\) Moreover, in the area of hate speech, the Commission has threatened to begin imposing mandatory regulations if companies’ self-regulation measures prove unsuccessful.\(^{221}\) Perhaps partially due to the implicit risk of further sanctions and regulation, American technology companies have complied readily with the requirements of the new GDPR.\(^{222}\) The combination of EU’s willingness to impose substantial fines, and technology companies’ apparent willingness to comply, suggests that American technology companies may be reluctant to violate GDPR terms after they become binding. This lends further support for the view that U.S. regulators need to be mindful of the competing requirements American companies face from European data protection regulators.

viii. Conflict of EU and U.S. Laws

The European data protection and U.S. regulators’ new disclosure rules may present severe conflict of laws problems for companies attempting to comply with both rules frameworks. The *U.S. v. Microsoft* case\(^{223}\) has shed some light on the possibility of this happening. Microsoft has argued that it cannot produce emails located on an Irish server sought pursuant to a U.S. court warrant because doing so would violate EU and Irish law.\(^{224}\) Both Microsoft\(^{225}\) and various amici\(^{226}\) have argued that extending the application of the SCA to apply extraterritorially to documents

---

\(^{219}\) GDPR, *supra* note 41, art. 83.


\(^{225}\) Id. at 1, 13.

located abroad would offend the sovereignty of those foreign governments. Several amici, including the European Commission, argue that in the context of criminal prosecution, courts seeking documents located in foreign jurisdictions should apply a comity framework, such as the one established in Société Nationale Industrielle Aérospatiale v. United States.\footnote{Id.; Brief for the European union as Amicus Curiae, supra note 206, at 6–7.}

A comity analysis certainly does not completely resolve the conflicting legal demands imposed on companies in the data protection context. Still, it provides an important principle for U.S. regulators to keep in mind in looking for workable solutions to the regulation of foreign political interference. This is consequential not just for ensuring sustained third country data transfers – it matters also for the business interests of the companies involved. For example, Microsoft has argued that if U.S. courts require American companies to produce documents in violation of foreign data-privacy laws, this will severely impact U.S. cloud-computing providers’ ability to operate in those jurisdictions by eroding foreign governments’ and consumer’s trust.\footnote{Brief for Respondent, supra note 224, at 57–58.}

ix. Harmonization of Data Protection Globally

Internet users and technology companies globally would benefit from greater harmonization of national and regional data protection regulations. Were the U.S. to adopt data protection regulations closer to those adopted by the EU, the legal uncertainty generated by issues such as third country data transfers would be greatly diminished. The legal certainty achieved by having consistent procedures for international data transfers more broadly would be in the advantage of businesses globally.\footnote{See Press Release, Open Forum Europe, Everyone Loses Out from Lack of Legal Certainty on Data Transfers (Oct. 7, 2015), http://www.openforumeurope.org/everyone-loses-out-from-a-lack-of-legal-certainty-on-data-transfers/ [https://perma.cc/Z5H2-XA9V]} While the implementation costs associated with the GDPR are significant for any individual company,\footnote{See, e.g., Mehreen Khan, Companies Face High Cost to Meet New EU Data Protection Rules, FIN. TIMES (Nov. 19, 2017), https://www.ft.com/content/0d47ff64-ccb6-11e7-7b81-794ce08b24dc [https://perma.cc/TED6-CGCJ] (estimating that compliance costs for Fortune500 companies are around $16 million and $550,000 for medium-sized companies).} the transaction costs and investment disincentives caused by uncertain and sometimes contradictory data protection regimes can be high and long-lasting,\footnote{See, e.g., UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, DATA PROTECTION REGULATION AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT (2016), http://unctad.org/en/PublicationsLibrary/dfsitstic2016d1_en.pdf [https://perma.cc/DZ7Q-5AX8] (discussing key business concerns from data protection).} and the conflict of law implications discussed above non-trivial.

Given that cross-border transactions and transfers are an integral feature of daily consumer and business usage, no regulatory framework based on purely national or regional approaches is likely to satisfactorily regulate internet usage.\footnote{Anupam Chander, Facebooksitan, 90 N.C. L. REV. 1807, 1841–42 (2012) (discussing different national and treaty-based ways of regulating Facebook and concluding that they all have significant flaws).} Global harmonization of data protection regulations is complex. Countries differ vastly in their philosophical and cultural approaches to the regulation of privacy, of which the
competing U.S. and European approaches are just two examples.

Nonetheless, this is a field where industry incentives may provide a push towards greater harmonization, e.g. through the presence of the so-called Brussels Effect.

There is a growing number of indications that Europe’s data protection regime could be exported to jurisdictions outside the EU, and thereby serve as a step towards greater data protection harmonization globally. Most recently, the Financial Times reported that the EU has agreed to include language in all its future trade agreements requiring its trading partners to enact robust data protection rules. This is a sign that the EU will prioritize data protection over trade. Moreover, even without explicit pressure, technology companies are beginning to implement EU-style data protection mechanisms beyond the EU. Facebook announced in January that it is introducing a privacy control center globally.

x. Implications for Regulation of Fake News

The policy recommendations discussed here center on the issue of paid political advertising. However, foreign political interference in U.S. elections extends well beyond paid advertising. For example, during the 2016 election cycle, over 120 million Americans were exposed to ordinary non-paid Facebook posts published by Russian individuals and entities. To the extent these posts contain propaganda or misinformation, they can be considered a part of the broader problem of “fake news.”

The regulation of fake news presents challenges distinct from those involving the regulation of political advertising, including whether online platforms like Facebook and Twitter should be protected by the first amendment, and whether

---

233 See supra Part I(A)(i) and accompanying discussion.
234 See, e.g., Data Protection: Brussels’ Heavy Hand on Europe’s Digital Economy, FIN. TIMES (Nov. 21, 2017), https://www.ft.com/content/777a1d34-cb4-11e7-b781-794ee06b24de [https://perma.cc/T2G9-5E4J] (arguing that “[t]he GDPR will also have an international dimension . . . [t]he regulation requires compliance from any company, even outside Europe, doing business with EU customers . . . . [t]hrough the so-called Brussels effect, where companies gravitate towards implementing the toughest rules they face, this is likely to spread restrictive practices through the world economy.”); see also Anu Bradford, The Brussels Effect, 107 NW. U. L. REV. 1, 68 (2012) (for background on the Brussels Effect).
235 Mehreen Khan & Jim Brunsden, EU to Demand Tough Data-Protection Rules With Future Trade Deals, FIN. TIMES (Feb. 9, 2018), https://www.ft.com/content/e489abb8-0dc5-11e8-8eb7-42857ea9b9 [https://perma.cc/98JA-QRCC].
238 See, e.g., Nabih Syed, Real Talk About Fake News: Towards a Better Theory for Platform Governance, 127 YALE L.J.F. 337, 337 (2017), (arguing that while “Fake News” eludes a common definition it is frequently construed as referring to “propaganda, misinformation, or conspiracy theories.”).
the government should have a part in regulating free political speech. Nevertheless, some of the challenges for regulating foreign political advertising also apply to the regulation of fake news on social media platforms. For example, were U.S. regulators to require disclosure of European social media accounts spreading misinformation about U.S. elections, GDPR rules concerning personal data transfer to third countries could limit whether that information could be shared with U.S. regulators or the public. Voluntary disclosure of personal data about European Union data subjects by social media platforms could also be limited by the GDPR. Therefore, U.S. efforts to regulate non-paid social media posts by foreign users will likely require similar cooperation between European and U.S. regulators.

CONCLUSION

The American effort to regulate foreign online political advertising centers on a crucial interest for American democracy: the ability to protect its electorate from malicious foreign interference. Yet, the regulatory effort also brings up fundamental questions about the value of privacy in the internet age. European efforts to regulate privacy may limit the efficacy of U.S. regulations.

Social media companies whose business models depend on user engagement and trust on both sides of the Atlantic are significant stakeholders in this debate. They may be caught in a difficult position when faced with conflicting demands from two powerful global regulators: the U.S. government’s push to regulate political speech on these platforms and EU’s effort to protect fundamental rights to privacy. This difficulty is not trivial – European regulators control access to an important market and could levy substantial fines. At the same time, compliance with American regulators’ demands is essential for ensuring the future development and existence of these platforms. These concerns illustrate the continued need for cooperation between EU and U.S. regulators in enacting comprehensive internet regulatory frameworks that can achieve the protection of both political integrity and data privacy, as well as enabling sustained Transatlantic data transfers.

Internet companies and users act in a fundamentally borderless forum but are currently faced with legal and regulatory frameworks that are national and regional in scope. The emergence of conflicting obligations, such as those discussed here, shows the extent to which greater harmonization of rules and regulations is necessary. Some of that harmonization is happening organically, in how social media companies are extending GDPR protections to users outside of the EU. However, these developments alone are not enough. Regulators on both sides of the Atlantic must ensure that the rules they impose move towards greater consistency.

241 See supra Part II(B)(ii) and accompanying discussion concerning third country data transfers.
242 See supra Part II(B)(iv) and accompanying discussion concerning confidentiality and public disclosures of personal data.