CHAIR ELLEN L. WEINTRAUB
FEDERAL ELECTION COMMISSION
WASHINGTON, D.C. 20463

Written Testimony of Chair Ellen L. Weintraub
Before the Subcommittee on National Security
Committee on Oversight and Reform
U.S. House of Representatives
May 22, 2019

Chairman Lynch, Ranking Member Hice, and members of the Committee, thank you for inviting me to testify on the topic of protecting the nation's election infrastructure from cybersecurity threats and disinformation campaigns.[1] I appreciate the Committee's forward-looking approach to these ongoing problems, especially as we head into the 2020 elections.

I have devoted my career to working to protect the integrity of our democracy. Throughout my years of service, I have not witnessed a graver danger to our political system than the current threat posed by foreign adversaries set on interfering with U.S. elections. Nor have I ever seen a moment where it has been more essential for Congress to bolster our nation's ability to combat attacks on our elections.

The U.S. Intelligence Community has made it clear that our foreign adversaries are launching cyber-attacks against our state election authorities.[2] The threat to America's election infrastructure, however, extends far deeper than computer-hacking operations. The basic, underlying framework of our system of elections – its infrastructure – is not just the brick-and-mortar electoral apparatus run by state and local governments. It is, more fundamentally, the faith that American citizens have in our elections. And that faith has been under malicious attack from our foreign foes through disinformation campaigns.

Our foes are trying to exacerbate tensions in our community, trying to drive us further apart. It is essential that we respond with our eyes wide open, by rejecting divisiveness, by coming together to fight these attacks for the good of the nation and our democracy. At the national level, Congress, the President, our national security agencies, and the FEC must ask

---

[1] I am testifying as the Chair of the Federal Election Commission. The opinions expressed are my own.

[2] *See generally* U.S. DEP'T OF HOMELAND SEC. & OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security* (Oct. 7, 2016), https://go.usa.gov/xmV6K; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *Assessing Russian Activities and Intentions in Recent US Elections* (Jan. 6, 2017), https://go.usa.gov/xmVFe; U.S. DEP'T OF JUSTICE, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election* (Mar. 2019), https://go.usa.gov/xmV6R.

ourselves: What can we do to protect all of America's political infrastructure from foreign interference?

One key task is keeping foreign money out of our elections. Federal campaign finance law already prohibits foreign nationals from making contributions to political campaigns,[3] but hidden money from foreign sources represents a significant vulnerability for American democracy.

We have seen how our foreign foes are willing to spend directly in our elections to destabilize them. I want to point out one particularly powerful and covert tool at our foes' disposal, one I believe they have yet to fully exploit: dark money. As we sit here today, a foreign adversary can transfer money to a 501(c) organization that can in turn contribute funds to a super PAC without disclosing the foreign source of money. A foreign-owned LLC can contribute to a 501(c) or a super PAC without those entities ever disclosing the true owners of the LLC.

The presence of dark money in campaign coffers can undermine the confidence that Americans place in our elections and our elected officials. At the moment, we do not know how much foreign dark money makes its way into our political campaigns, but we do know that the doors are wide open for political money to be weaponized by well-funded hostile powers.[4]

Even fully disclosed money spent by U.S. corporations with foreign parents raises concerns about foreign influence. When a U.S.-based company is owned by foreigners, the U.S. managers are obliged to spend company resources in a way that best serves the interests of the foreign owners, not the American people. I have proposed rulemakings that would address these concerns, but these efforts have so far been blocked at the FEC.[5] Even my proposal to address spending in our elections by companies that are *wholly owned by foreign governments* was rejected.[6] Until we address, by statute or regulation, the various ways that foreigners may route money through corporate entities, our political system remains at risk of being influenced by foreign corporate or governmental interests. The idea behind regulating foreign-owned entities is not novel. The federal government already does it in the context of communications law and

---

[3] The Federal Election Campaign Act of 1971, as amended, ("FECA" or the "Act") broadly prohibits foreign nationals from directly or indirectly making contributions or donations of money or other things of value in connection with any federal, state, or local election. 52 U.S.C. § 30121.

[4] *See, e.g.*, Neil Barnett & Alastair Sloan, *Democracy in the Crosshairs: How Political Money Laundering Threatens the Democratic Process*, ATLANTIC COUNCIL (Sept. 2018), http://bit.ly/2LQ8g6Z.

[5] *See, e.g.*, Comm'r Ellen L. Weintraub, *Rulemaking Proposal to Combat Foreign Influence in U.S. Elections*, FEDERAL ELECTION COMMISSION (May 17, 2018), https://go.usa.gov/xmvE4; Comm'r Ellen L. Weintraub, *Revised Proposal to Launch Rulemaking to Ensure that U.S. Political Spending is Free from Foreign Influence*, FEDERAL ELECTION COMMISSION (Sept. 28, 2016), https://go.usa.gov/xmVAt.

[6] Minutes, Federal Election Commission Open Meeting of May 24, 2018, at 10, https://go.usa.gov/xmvdj.

securities law.[7] We already scrutinize foreign investments in U.S. companies or operations that implicate our national security interests.[8] Our elections should be similarly protected.

These are not hypothetical concerns. Take one of our recent enforcement actions, for example, in which the Commission levied record fines against a super PAC and a number of individuals – including foreign nationals – that orchestrated the donation of $1.3 million from foreign nationals to a super PAC supporting a 2016 presidential candidate.[9] These contributions were funneled into our political system through a foreign-owned subsidiary operating in the United States. This is just one way that foreign nationals are making their influence felt at even the highest levels of our political campaigns.

These kinds of cases are increasingly common. From September 2016 to April 2019, the number of matters before the Commission that include alleged violations of the foreign-national contribution ban increased from fourteen to forty. There were thirty-two matters open as of April 1, 2019. The Commission has committed to prioritizing enforcement matters that allege violations of the foreign national prohibition, and the division responsible for prosecuting these enforcement actions currently takes a number of steps to fast-track these cases.

Despite these efforts, however, the ability to move quickly on enforcement matters is hampered by historically low enforcement-staff levels. Our lawyers are scrambling to keep up with the workload. Plus, two commissioner positions are vacant, one for more than a year and the other for more than two years. The four affirmative votes required to take action in these foreign national cases require unanimous support from a Commission that often does not see eye-to-eye on its enforcement mission. While it is good that we were able to muster the necessary unanimity to address the outrageous conduct in the case described above, that level of agreement is too rare. To keep foreign money out of our elections, we need a full complement of FEC commissioners and staff. Until that happens, we are hobbled in our ability to enforce the law.

Another key task is to respond to the changing nature of political campaigns that are increasingly being conducted over the internet and social media. The Commission is responsible for ensuring that the American public remains informed about who is behind the political communications that inform their votes. That task is changing rapidly. More and more Americans rely on the internet and mobile devices to obtain information. Spending on digital political ads during the 2018 midterm election increased by 260% from the 2014 midterm

---

[7] *See, e.g.*, 47 U.S.C. § 310(a)-(b) (restricting foreign ownership of radio stations); 15 U.S.C. §§ 80a-1 *et seq.* (restricting certain sales of securities and imposing registration requirements).

[8] 50 U.S.C. § 2170(a).

[9] Statement of Reasons of Chair Ellen L. Weintraub, MUR 7122 (Right to Rise USA, *et al.*) (Apr. 12, 2019), https://go.usa.gov/xmdAK.

election, to roughly $900 million.[10] Digital ad spending in the United States may grow to nearly $130 billion in 2019, representing over half of the total estimated ad spending in the country.[11]

Congress and the FEC must respond to foreign disinformation campaigns that have proliferated online. For my agency to do so, the FEC needs better tools from Congress so that we can get a handle on the advertising dollars that are pouring into the social-media networks. Online political manipulation can take many forms: disinformation, political botnets, fake social media accounts, troll farms, and paid digital advertising. I have written about these dangers before, and while today's cybersecurity threats are complex problems requiring a multifaceted response, one easy place to start is with more robust disclosure requirements for online political advertising.[12] At a minimum, digital advertising should be subject to the same disclosure and disclaimer requirements as broadcast advertising. The Honest Ads Act would be a very good first step.[13]

The public's interest in this problem has grown along with the threat. When the Commission first proposed a rulemaking about internet disclaimers several years ago, we received eight comments. The Commission re-opened the comment period for this rulemaking in 2017 and 2018, receiving more than 314,000 comments combined.[14] The Commission held a two-day public hearing on June 27 and 28, 2018.[15] We held two further information sessions on July 30, 2018, and August 27, 2018. Last year's notice of proposed rulemaking contained several proposals, and based on the information we received, I made a modified proposal to my colleagues last fall. We have had some informal discussions, but I have yet to receive a concrete counter-proposal. I am very sorry to report that it is not at this time clear whether there will be four affirmative votes to adopt a final rule.

Some of the social media platforms have attempted to step into the void with their own improved disclaimer and disclosure regimes for political advertising. This is to their credit, but it has not been without controversy. Questions have arisen, such as: What triggers the requirement to post a disclaimer? Can the disclaimers be relied upon to honestly identify the sources of the digital ads?[16] Does identifying information travel with the content when information is

---

[10] Sara Fischer, *Political Ad Spending Hits New Record for 2018 Midterm Elections*, AXIOS (Nov. 6, 2018), http://bit.ly/2WSlXmQ.

[11] *US Digital Ad Spending Will Surpass Traditional in 2019*, EMARKETER (Feb. 20, 2019), http://bit.ly/2EjB7KI.

[12] Ellen L. Weintraub, *Our Elections Are Facing More Threats Online. Our Laws Must Catch Up*, WASH. POST (Sept. 14, 2017), http://wapo.st/2eZbQs3.

[13] The Honest Ads Act alone is necessary but not sufficient to address foreign interference in our elections. Notably, legislation such as the Secure Elections Act and the DETER Act have bipartisan support and are also urgently needed.

[14] *See* Internet Communication Disclaimers, 83 Fed. Reg. 12,864 (Mar. 26, 2018), https://go.usa.gov/xmVHe.

[15] *See* Agenda, June 27-28, 2018, Public Hearing: Internet Communication Disclaimers and Definition of "Public Communication," https://go.usa.gov/xmVHt.

[16] *See* William Turton, *We Posed as 100 Senators to Run Ads on Facebook. Facebook Approved All of Them*, VICE NEWS (Oct. 30, 2018), http://bit.ly/30w6FXf.

forwarded? How are the platforms to deal with the transmission of encrypted information? Peer-to-peer communications present a burgeoning field for political activity, raising a new set of potential issues. Whatever measures are adopted today run the serious risk of targeting the problems of the last cycle, not the next one.

In addition to more robust advertising disclosure requirements, we must consider cybersecurity countermeasures for political campaigns. Campaign cybersecurity is essential, but efforts to put these in place are in their early stages and face significant hurdles. In the wake of campaign-related cyber-attacks that have targeted Democratic and Republican campaigns alike, security companies, technology companies, and nonprofits have considered offering free or discounted cybersecurity products and services to political campaigns. These offers pose complications for political campaigns, however, because campaign finance regulations prohibit corporations from donating directly to campaigns. This prohibition applies to in-kind contributions such as free or discounted cybersecurity services. The Commission is currently considering whether to allow a nonprofit to provide free or discounted cybersecurity services.[17] It is a proposal that I am seriously considering approving through a tailored advisory opinion, but this is a problem that would benefit from a legislative solution. I am also proposing an interpretive rule that would allow national party committees to use their building funds to pay for cybersecurity expenses for themselves, state parties, and candidates.

* * *

Our elections are under attack. To defend America's democracy, Congress and the FEC must do more to mitigate the discord sown by foreign interference on and off the internet. Congressional efforts to safeguard U.S. elections from foreign interference must take into account the broader electoral infrastructure that includes political campaigns and political discourse. The threat we face to the underlying framework of our political system includes dark money that may be hiding foreign sources and the manipulation of the online political community in which we increasingly conduct our political debates.

Serious thought has to be given to the impact of social media on our democracy. Facebook's philosophy of "Move Fast and Break Things," cooked up sixteen years ago in a college dorm room, has breathtaking consequences when the thing they're breaking could be democracy itself. Facebook, Twitter, WhatsApp, Google – these and other technology giants have revolutionized the way we access information and communicate with each other. Social media has the power to foster citizen activism, virally spread disinformation or hate speech, shape political discourse. Government cannot avoid its responsibility to scrutinize this impact.

The Legislative and Executive Branches must step forward on a bipartisan basis to address the full range of cyber threats to our democracy. I commend the Committee for convening this hearing and placing a spotlight on these critical issues. The 2020 election is around the corner. The time to act is now.

---

[17] Request, Advisory Op. 2018-12 (Defending Digital Campaigns, Inc.) (Sept. 6, 2018), https://go.usa.gov/xmvyY.