About the Brennan Center for Justice

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize — and when necessary defend — our country’s systems of democracy and justice. At this critical moment, the Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

About the Brennan Center’s Liberty and National Security Program

The Brennan Center’s Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy, ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat, and securing adequate oversight and accountability mechanisms.

About the Brennan Center’s Publications

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

Acknowledgments

The authors are grateful to Michael Waldman for his vision in developing An Election Agenda for Candidates, Activists, and Legislators; Vivien Watts and John Kowal for their insights and support; and Andrew Lindsay, Michael German, Harsha Panduranga, and Erica Posey for their research and drafting contributions. They also thank Yuliya Bas, Lisa Benenson, Naren Daniel, Trip Eggert, Stephen Fee, Theresa Jefferson, Jim Lyons, and Alden Wallace for their editing and communications assistance.

© 2018. This paper is covered by the Creative Commons Attribution-NonCommercial-NoDerivs license. It may be reproduced in its entirety as long as the Brennan Center for Justice at NYU School of Law is credited, a link to the Center’s web pages is provided, and no charge is imposed. The paper may not be reproduced in part or in altered form, or if a fee is charged, without the Center’s permission. Please let the Center know if you reprint.
About the Authors

Faiza Patel serves as co-director of the Brennan Center’s Liberty and National Security Program, which seeks to ensure that our counterterrorism laws and policies respect constitutional values, and promotes transparency and accountability in national security matters. She has testified before Congress opposing the dragnet surveillance of Muslims, developed legislation to create an independent inspector general for the New York Police Department, and organized advocacy efforts against anti-Muslim laws and policies. She has authored and co-authored eight reports: Extreme Vetting and the Muslim Ban (2017), Trump-Russia Investigations: A Guide (2017), The Islamophobic Administration (2017), Countering Violent Extremism (2017), Overseas Surveillance in an Interconnected World (2016), What Went Wrong with the FISA Court (2015), Foreign Law Bans (2013), A Proposal for an NYPD Inspector General (2012), and Rethinking Radicalization (2011). She is a member of the Board of Editors of the legal blog Just Security. Born and raised in Pakistan, Patel is a graduate of Harvard College and the NYU School of Law.


Michael W. Price served as senior counsel for the Brennan Center’s Liberty and National Security Program. He worked to oppose discriminatory surveillance practices, developed legislation to create an independent inspector general for the New York Police Department, and authored numerous amicus briefs on behalf of the Brennan Center and others in cases involving electronic surveillance and privacy issues. He is the author of National Security and Local Police (2013) and Rethinking Privacy: Fourth Amendment “Papers” and the Third-Party Doctrine (2016). Before joining the Brennan Center, Price was the National Security Coordinator for the National Association of Criminal Defense Lawyers, where he provided legal assistance for the defense of detainees in the military commissions at Guantanamo Bay. Price also engaged in litigation and public advocacy on issues related to privacy, electronic searches and surveillance, and government secrecy. He holds a J.D. from NYU School of Law and a B.A. from Columbia University in Political Science and Middle East & Asian Languages and Cultures.
**Foreword**

How can we fix American government? How can we make sure it works for all?

In the wake of the convulsive 2016 election, there may be no more pressing question.

Nor will 2016 likely be the last such eruption. American politics has stagnated for years, locked in arid debate on old ideas. Political parties have become increasingly tribal. Elections are drenched in money and marked by intense polarization. Government dysfunction has created an opening for racially divisive backlash politics, while ignoring long-range economic, social, and environmental challenges.

Until we reckon with that public discontent, we’ll continue to be entangled in the same battles we’ve been fighting for decades.

It is time for fresh thinking, which is why the Brennan Center for Justice is producing Solutions 2018, a series of three reports setting out democracy and justice reforms that are intended to help break the grip of destructive polarization.

This volume sets out proposals to protect constitutional freedoms, vulnerable communities, and the integrity of our democracy amid new threats. Others will show how we can ensure free and fair elections, curb the role of big money in American politics, and end mass incarceration.

We hope these proposals are useful to candidates, officeholders, activists, and citizens. The 2018 election should be more than a chance to send a message. It should be an opportunity to demand a focus on real change.

What counts is not what we are against, but what we are for.

Michael Waldman  
*President*
# Table of Contents

Introduction ........................................................................................................ 1  
End Targeting of Minority Communities .......................................................... 2  
Stop Funding the “Muslim Ban” and “Extreme Vetting” ................................. 4  
End Warrantless Spying on Americans ............................................................. 6  
Protect Whistleblowers and the Press ............................................................... 8  
Protect Investigations into Russian Meddling in the 2016 Election .......... 10  
Conclusion ....................................................................................................... 12  
Endnotes .......................................................................................................... 13
Introduction

Americans need not choose between security and freedom. But the politics of fear and racial bias have too often supplanted sound policies. Instead of narrowly targeting actual threats to our safety and security, some law enforcement and intelligence policies broadly target entire communities, compromising the rights of law-abiding citizens and immigrants.

Practices such as racial profiling, warrantless spying, and callous immigration enforcement are key examples. They do nothing to keep us safe. Yet they erode the nation’s values and sow division. National security is used as a flimsy pretext to keep important details about such policies secret. In the meantime, efforts to thwart real threats to our security — such as Russia’s interference in our democratic process — are falling victim to politics.

As Americans, we can, and must, do better. This report offers five solutions to reform corrosive national security and law enforcement practices that fail to address actual threats to public safety. These proposals will rebuild public trust to enhance security, a goal that all lawmakers should support. A commonsense framework for national security for the 21st century would consist of the following actions:

• **End targeting of minority communities.** Congress should pass the End Racial Profiling Act, which would prohibit profiling based on race, religion, national origin, religion, gender, gender identity, or sexual orientation.

• **Stop funding the “Muslim ban” and “extreme vetting.”** Congress should cut all funding associated with President Donald Trump’s “Muslim ban” and “extreme vetting” policies, including the National Vetting Center.

• **End warrantless spying on Americans.** Congress should refresh privacy rules enacted before the World Wide Web to ensure Americans’ most private communications are protected. It should also enact reforms to ensure that warrantless surveillance ostensibly directed at foreigners isn’t used to spy on Americans.

• **Protect whistleblowers and the press.** Robust legal protection is especially important in an era when the president has dubbed broadcast networks “the enemy of the American people.” Congress should pass a “reporter shield law” to protect journalists, along with meaningful safeguards for national security whistleblowers.

• **Protect investigations into Russian meddling in the 2016 election.** Congress should pass legislation to ensure that special counsel Robert Mueller cannot be fired without cause and judicial review. Lawmakers should also conduct robust fact-finding inquiries to adequately address the threat of foreign interference in U.S. elections.

These proposals are practical solutions that reject the false choice between liberty and security. They promote the values and constitutional principles that define America. And they offer principles and policies that candidates of any party can and should support.
End Targeting of Minority Communities

Law enforcement profiling on the basis of race, religion, ethnicity, and the like is ineffective, degrading and counter to American values. It does not work.1 It stigmatizes entire communities.2 It harms trust in the police.3 And it perpetuates discrimination and bias among the general public.4

There is still no federal law against racial profiling, despite the Constitution’s core promise of equal protection under the law. Law enforcement agencies should investigate people because their conduct raises suspicion, not their racial or religious identity. But when it comes to immigration, national security, and intelligence activities, agencies set their own policies, which are full of loopholes permitting federal agents to engage in otherwise unlawful profiling. It is time for Congress to step in and finally pass legislation to close these loopholes, and end targeting of immigrant and minority communities.

The Department of Justice issues profiling guidelines that apply to several agencies. In 2014, following national outrage at police killings of black men in Ferguson, Mo., and New York City, the department expanded the general policy against racial profiling to include profiling based on ethnicity, gender, national origin, religion, sexual orientation, and gender identity.5 This was a welcome improvement, but the department’s policy kept carve-outs for national security and intelligence investigations, as well as Immigration and Customs Enforcement, Customs and Border Protection, and the Transportation Security Administration.6 The revised guidelines also did not apply to state and local law enforcement directly or provide for sufficient enforcement of the rules at the federal level.

Moreover, internal policies issued by the Federal Bureau of Investigations (FBI) and the Department of Homeland Security undermine the general rule against profiling in various ways.7 The FBI, for example, uses race, religion, and ethnicity for intelligence purposes and community “mapping.”8 It has also singled out so-called “Black Identity Extremists” for scrutiny based on the noxious notion that “perceptions of unjust treatment of African-Americans … will inspire premeditated attacks against law enforcement.”9 And the Department of Homeland Security uses nationality and religion as a factor in screening, investigations, and border patrol activities.10 In a clear instance of profiling based on religion, gender, and national origin, a draft department report from January called for long-term surveillance of Sunni Muslim immigrants with “at-risk” demographic profiles — i.e., those who are young, male, and from the Middle East, South Asia, or Africa.11

Clearly, current rules are too weak. It is long past time for Congress to pass legislation to prohibit discriminatory profiling by law enforcement — federal, state, tribal, and local — in all its pernicious forms.
• **Policy: Pass the End Racial Profiling Act**

Congress should pass the End Racial Profiling Act, H.R. 1498, and the End Racial and Religious Profiling Act, S. 411 (collectively referred to as ERPA), which have been introduced by Rep. Sheila Jackson Lee (R-Texas) and Sen. Ben Cardin (D-Md.), respectively. The law would create a uniform definition of racial profiling that applies to all levels of law enforcement. Specifically, it would expand the Justice Department’s criteria to include “actual or perceived” race, religion, national origin, gender, gender identity, or sexual orientation. Under ERPA, law enforcement could not rely on any of these characteristics, to any degree, in routine investigatory activities — including “stop and frisk” searches, criminal investigations and intelligence gathering, immigration-related workplace investigations, vehicle searches, and border inspections or interviews.

ERPA would also make the ban on racial profiling enforceable. It would allow individuals injured by racial profiling to sue law enforcement to compel compliance with the statute. Critically, it would link popular Justice Department grants to compliance. Every state in the country receives federal funds for their state, local, and tribal law enforcement activities; to continue receiving this money, ERPA would require them to adopt and follow policies and procedures designed to eliminate racial profiling. Furthermore, ERPA would create data collection and reporting requirements used to verify compliance or identify unlawful profiling.

The rules would include appropriate privacy protections while providing a critical tool to increase accountability.

Both Presidents Bush and Obama have supported legislation to end racial profiling. According to President Bush, reform was necessary because, “Too many of our citizens have cause to doubt our nation’s justice when the law points a finger of suspicion at groups instead of individuals.” Congress has allowed ERPA to languish, but should now act with urgency.

Americans overwhelmingly oppose racial profiling. And at a time when racism, xenophobia, and Islamophobia flow from the White House daily, elected leaders should take a stand and protect the rights of all Americans by supporting ERPA.
President Trump’s “Muslim ban” has been devastating for American Muslims — stigmatizing entire communities, hurting families, and stoking the flames of religious hatred. It also harms tourism, the technology industry, universities, medical institutions, and ultimately, tax revenues.23 Multiple federal courts have found that the ban likely violates immigration law and the Constitution’s edict that government may not favor one religion over others.24 Using the president’s own disparaging tweets as evidence, the Fourth Circuit Court of Appeals ruled that the ban is “unconstitutionally tainted with animus toward Islam” and strikes at the basic notion of religious liberty.25 Nonetheless, the Supreme Court allowed the ban to go into full effect while legal challenges are under way.26

“Extreme vetting” is the “Muslim ban’s” pernicious companion. It subjects visa applicants to an unnecessary multiagency security review process based solely on their national origin, using criteria drawn directly from the “Muslim ban.” Applicants must submit more personal information than is needed to get a Top Secret security clearance, including their social media data, often delaying their applications for months.27

Additionally, Immigration and Customs Enforcement intends* to feed such data into a computer algorithm, developed by outside companies, that will supposedly predict whether applicants will “become a positively contributing member of society” or commit terrorist acts.28 This “extreme vetting” by algorithm is not just for initial screening, but also for ongoing monitoring of social media and location information while travelers are in the United States.29

The program would continuously scour the internet, including “media, blogs, public hearings, conferences, academic websites, social media websites such as Twitter, Facebook, and LinkedIn,”30 hunting for any “derogatory” information and helping Immigration and Customs Enforcement to “locate and detain” people.31 It would almost certainly sweep in information about American citizens who happen to be communicating with an immigrant or visitor.32

This type of social media monitoring can chill free expression and is ripe for discrimination.33 It is not justified by any security benefit. The U.S. already has an extremely strict and successful vetting process, and “extreme vetting” would add little value.34 Technologists widely agree that no computer algorithm can predict who will

* In May 2018, Immigration and Customs Enforcement, under pressure from the Brennan Center and others, reportedly abandoned efforts to build a social media vetting algorithm, though it still intends to monitor social media in a variety of ways.
commit a terrorist act, let alone who will “positively contribute” to society. Indeed, “extreme vetting” appears to be less a national security measure, and more a convenient way to curb the flow of legal immigrants and visitors to the country — an explicit goal of this administration, despite the tremendous economic and cultural contributions immigrants make to the United States.

Despite objections, President Trump is doubling down on these misguided proposals. He recently ordered the creation of a “National Vetting Center” to help implement “extreme vetting.” The State Department is expanding social media monitoring, potentially reaching 140 million visitors to the United States. But Congress can put a stop to these pernicious practices.

- **Policy: Defund the “Muslim Ban”**
  Lawmakers should begin by defunding all activities relating to the “Muslim ban.” There are bills in the House of Representatives and Senate to do just that — H.R. 4271, introduced by Rep. Judy Chu (D-Calif.), and S. 1979, introduced by Sen. Chris Murphy (D-Conn.) (both titled “A bill to block the implementation of certain presidential actions that restrict individuals from certain countries from entering the United States”). They would withhold federal funding to enforce the ban and also declare it illegal under the Immigration and Nationality Act of 1965, which prohibited discrimination on the basis of national origin.

- **Policy: Prohibit Social Media Monitoring for “Extreme Vetting”**
  Lawmakers should prohibit Immigration and Customs Enforcement from implementing social media monitoring programs for “extreme vetting” purposes — at least until the agency has demonstrated their usefulness, and explained how it intends to protect privacy and free speech. These programs chill free expression and enable discrimination without any countervailing security benefit. Indeed, according to Department of Homeland Security’s own inspector general, they “lack criteria for measuring performance to ensure they meet their objectives.”

- **Policy: Do Not Fund the National Vetting Center**
  Lawmakers should ensure that not a dime of taxpayer money goes to construct or operate the National Vetting Center as long as “extreme vetting” remains its ostensible purpose.

Americans support religious liberty. They are sick of divisiveness. Candidates should understand the alarm of many Americans at the animus President Trump has shown American Muslim and immigrant communities. This is a country founded by immigrants who valued religious freedom. Candidates should stand up for the values Americans hold dear, and use every tool at their disposal to stop the “Muslim ban” and “extreme vetting.”
End Warrantless Spying on Americans

Warrants are one of the most basic safeguards of American democracy. The Revolution was fought, in part, because of colonial revulsion toward abusive searches and seizures by British agents. In fact, the Founders regarded warrants as one of the key elements of American law, a barrier to government overreach and guardian of individual liberty.

Warrants keep the government out of our private affairs unless there is a compelling need and court supervision, protecting dissent and free speech as well as the privacy of political, religious, and social activities. But the law has not kept pace with rapid changes in technology or with the government’s actual surveillance practices. As a result, privacy protections are steadily eroding.

Many of the laws protecting online privacy are older than the World Wide Web. A warrant is required to open postal mail or intercept a telephone call, but different standards apply to emails, text messages, location data, and other electronic files stored in the “cloud.”

The privacy of digital communications depends on the Electronic Communications Privacy Act (ECPA), a law that has not been meaningfully updated since it was passed in 1986 — when the personal computer was in its infancy, and Mark Zuckerberg was 2 years old. ECPA requires a warrant only for emails that are unread and less than 180 days old — a hopelessly arbitrary rule in today’s world, as some courts have begun to recognize. It also does not require a warrant for “metadata,” or information about digital communications, including internet browsing history and search queries, to/from information, or cellphone location records. As a result, some of our most private digital data receive less protection than physical junk mail, just because they involve technologies that Congress never anticipated. This is out of step with the way Americans communicate today. It is bad for privacy and bad for business.

Compounding the problem, the National Security Agency continues to conduct warrantless mass surveillance of foreigners’ internet communications, vacuuming up enormous amounts of Americans’s data in the process. Section 702 of the Foreign Intelligence Surveillance Act, passed in 2008, permits the agency to conduct warrantless surveillance of foreigners outside the country, regardless of whether they are suspected of any wrongdoing. This surveillance inevitably ensnares Americans’s emails and phone calls — including communications with, or simply about, foreigners being surveilled. It could also collect any communications that even mention Islamic State group or any number of foreign leaders and public figures.
But instead of protecting Americans’s constitutional rights by deleting these “incidentally” acquired exchanges, the NSA holds on to them for years. Worse, the FBI is allowed to search and read these communications by Americans without any evidence of criminal activity, let alone probable cause and a warrant. Lawmakers recently missed a critical opportunity to stop this practice. Section 702 was set to expire this year, but Congress reauthorized it until 2023 without adding meaningful privacy protections. Americans need a privacy upgrade.

Policy: Modernize ECPA
Privacy laws for the digital age are long overdue. Lawmakers should modernize ECPA to protect Americans’s privacy rights in the 21st century, making it clear that the warrant standard applies to personal data just as it applies to personal property. The bipartisan ECPA Modernization Act would take a key step in that direction by requiring a warrant for cloud data and geolocation information.

Specifically, the ECPA Modernization Act (S. 1657), introduced by Sens. Mike Lee (R-Utah) and Patrick Leahy (D-Vt.), would require a warrant for communications and other types of content stored in the cloud, such as emails, texts, or photos kept with third-party companies like Google, Apple, or Microsoft. A complementary bill on email privacy has already passed the House, the Email Privacy Act (H.R. 387) introduced by Rep. Kevin Yoder (R-Kan.). The ECPA Modernization Act would also require a warrant to obtain the location information that today’s smartphones constantly create, including GPS data and cellphone location records held by third-party service providers like AT&T, Verizon, and Sprint.

Lawmakers should consider adding another critical protection: a warrant requirement to obtain other forms of “metadata” — details about where, when, how, and with whom we communicate online — that can be just as revealing as actual content.

Policy: Fix FISA Section 702
Rather than reforming Section 702 when it came up for reauthorization in 2017, Congress narrowly voted to extend the law until 2023. But the ongoing intrusion into Americans’s privacy cannot be allowed to continue for another six years.

Lawmakers should enact legislation that would require the government to obtain a warrant before combing through NSA data looking for Americans’s communications. Reps. Ted Poe (R-Texas) and Zoe Lofgren (D-Calif.) introduced a bill along these lines that passed the House in 2014 and 2015. They offered a similar bill, which also would have prohibited the collection of communications that merely mention people or groups who have been targeted for surveillance, as an amendment during the 2017 reauthorization debate, but it never received a vote. Both houses of Congress should now take up this legislation and pass it.

Members of both parties are concerned about protecting privacy. Americans do not want the government peering inside their computers or tracking their location via a cellphone any more than they want a hidden microphone planted under their kitchen table. Tech giants like Microsoft, Google, and Apple have also thrown their support behind reforms, imploring Congress to keep pace with technological advances. It is well past time for lawmakers to act on these concerns, ensure that warrants remain a foundational check against government overreach, and provide Americans with privacy protections that are equal to the government’s ability to look into their private lives.
President Trump continues to attack the press with extraordinary intensity and ire. At least one Republican
critic of Trump, Sen. Jeff Flake (R-Ariz.), who is retiring from the Senate after a single term, delivered a
blistering critique of Trump’s stance from the Senate floor. The president’s “unrelenting daily assault on the
constitutionally-protected free press…[is] as unprecedented as it is unwarranted,” Flake said.53

Since declaring his candidacy in June 2015, Trump has racked up roughly 1,000 tweets critical of the press —
which works out to an average of one per day. Some of these tweets have used violent imagery, including one
doctored to show the president wrestling and punching a CNN logo.54 Trump has repeatedly called for official
retaliation against the press for unfavorable coverage, including congressional investigations into “Fake News
Networks,” the repeal of broadcast licenses, and the jailing of journalists.55 He also wants to make it easier
to sue for libel.56 In the president’s own words, media outlets deemed “fake” — including NBC, ABC, CBS,
CNN, and The New York Times — are the “enemy of the American people.”57

The administration has also promised to crack down on leaks, with potentially dire consequences for
whistleblowers who disclose information about government waste and abuse, and journalists who publish that
information. At a news conference in September 2017, Attorney General Jeff Sessions announced that the
Justice Department “has more than tripled the number of active leak investigations” since the end of the Obama
administration.58 Moreover, he did not rule out jailing reporters for not revealing their sources, especially in the realm of national
security. “We respect the important role that the press plays, and we’ll give them respect, but it not unlimited,” Sessions said. Indeed, the
Trump administration is trying to roll back enhanced protections for
reporters that were issued by the Obama Justice Department after a
debacle in which the department seized the Associated Press’s phone
records as part of a leak investigation.59

Congress should step in and codify protections for journalists and
their sources. Whistleblowers are essential to making sure that government wrongdoing does not go unnoticed.
Proposals to protect the press and whistleblowers enjoy broad bipartisan support and would help restore trust in
public institutions.

• **Policy: Pass a “Reporter Shield Law”**

  Lawmakers should pass a “reporter shield law” that would limit the circumstances under which the
government can demand information from journalists or compel the disclosure of data from a third-party
communications service provider, such as a cellphone company.60 Every state but Wyoming has some form of
shield law, also known as “reporter’s privilege.”61 Such a law would make it easier for federal officials to share

---

**Protect Whistleblowers and the Press**

Whistleblowers are essential to making sure that government wrongdoing does not go unnoticed.

---
information of public interest with journalists, and would give reporters the freedom they need to conduct their constitutionally protected role of government oversight.\textsuperscript{62}

Press shield laws have passed the House of Representatives and the Senate Judiciary Committee with bipartisan support.\textsuperscript{63} Indeed, as a congressman, Vice President Mike Pence was a fierce advocate for a federal reporters’ privilege.\textsuperscript{64} In the current Congress, representatives on opposite ends of the political spectrum, including Reps. Jamie Raskin (D-Md.) and Jim Jordan (R-Ohio), have come together to co-sponsor the Free Flow of Information Act (H.R. 4382), which is now in committee.\textsuperscript{65} Unfortunately, the bill contains too many exceptions, including an overbroad carve-out for national security. Congress should strengthen the bill to provide a broad definition of journalists, and back only narrow exceptions for criminal prosecution and national security.

\textbf{• Policy: Protect Whistleblowers}

Congress should do more to protect whistleblowers — especially those within the intelligence community, who lack statutory protection against retaliation.\textsuperscript{66} In fact, intelligence community contractors now enjoy more robust protections than those available to intelligence community employees, owing to changes made to the law in January.\textsuperscript{67} Moreover, the FBI has its own internal rules for whistleblowing. According to both the Government Accountability Office and former FBI agents, these rules fail to ensure timely, fair, and independent resolution of whistleblower claims.\textsuperscript{68} Both Republican and Democratic senators continue to press the issue of protecting whistleblowers, including those from the FBI.\textsuperscript{69}

A free press and the ability for government officials to bring official misconduct to light are essential for our democracy and our security.\textsuperscript{70} A strong press shield law and statutory whistleblower protections for intelligence employees would be important steps toward promoting a government accountable to the people.
The investigations into Russian interference in the 2016 U.S. election are among the most important inquiries in American history: they bear on the integrity of American democracy itself. Instead of backing these probes, the president has tried to thwart them at every turn, potentially to the point of obstructing justice. Congress can and should act to protect the independence of special counsel Robert Mueller’s investigation to preserve public trust in our elections and the rule of law. And lawmakers should exercise their own fact-finding powers to ensure a robust role for Congress in the investigatory process.

There are two efforts now underway: one investigation led by special counsel Robert Mueller, and another led by the Senate Intelligence Committee. A third investigation, by the House Intelligence Committee, concluded that there was no “collusion” between Russia and the Trump campaign. But the House investigation ended early, was divided along partisan lines, failed to obtain key information from witnesses, and contradicted the entire intelligence community on Russia’s motivation for meddling.

It is no secret Trump wants the investigation into Russian interference with the 2016 election to vanish. The president fired FBI director James Comey — and ironically triggered the appointment of Mueller — in an attempt to shut it down. “In fact, when I decided to just do it [fire Comey], I said to myself, I said, ‘You know, this Russia thing with Trump and Russia is a made-up story, it’s an excuse by the Democrats for having lost an election that they should have won,’” Trump famously told NBC News about a week before Mueller was appointed. He then publicly criticized the deputy attorney general, Rod Rosenstein, for appointing Muller as special counsel, and derided the entire investigation as a “Witch Hunt.” Trump even ordered Mueller’s firing outright, backing down only after the White House counsel threatened to resign.

Anyone concerned about the integrity of elections and the rule of law should be worried that the president will continue to look for ways to fire Mueller and stop the investigation, either by pressuring Justice Department officials or firing them one-by-one in a slow-motion replay of President Nixon’s “Saturday Night Massacre.” But members of Congress can do more than worry. Legislators are not spectators: Congress can act to protect Mueller’s independence, and it can also conduct its own investigations.

- **Policy: Pass Legislation Protecting Mueller’s Investigation**
  Bipartisan legislation, introduced in the Senate, would codify existing Justice Department rules that bar removing a special counsel absent good cause. Without such a law, the Justice Department could rescind those rules unilaterally.
The bill is called the Special Counsel Independence and Integrity Act, introduced by Sens. Lindsey Graham (R-S.C.), Chris Coons (D-Del.), Thom Tillis (R-N.C.), and Corey Booker (D-N.J.). To safeguard independent investigations, the proposal requires notice of the reason for a special counsel’s removal, and provides an opportunity for a panel of federal judges to prevent a removal from taking effect if they determine it was not for good cause. During judicial review, an investigation would remain staffed and its materials preserved.

**Policy: Continue Congressional Investigations**

Lawmakers should also pledge to continue investigating Russian interference in U.S. elections. Unlike Muller’s investigation, which is focused on criminal conduct, congressional committees can use their fact-finding authority to uncover additional information about noncriminal conduct that may still have important implications for national security and our electoral system. While the House investigation was a blatant political whitewash, the Senate Intelligence Committee’s investigation has taken place largely out of the public eye, making it difficult to assess its adequacy. Lawmakers should publicly insist that this investigation be as robust and wide-ranging as possible. If the committee’s effort ultimately comes up short, the next Congress can and should reopen these investigations.

The American people deserve to know the extent to which Russian agents intervened in the 2016 election, and whether their actions were assisted by anyone inside the United States — including the president. No less than the integrity of our democracy is at stake.
Conclusion

Americans want leaders who will protect their safety and their rights. That means focusing our efforts on true threats to national security, such as Russia’s interference with the U.S. electoral process, and not using our law enforcement and intelligence resources to target racial or religious minorities, or to invade the privacy of all Americans.

The above proposals provide candidates of all stripes with a commonsense approach to liberty and security. They provide a path forward that will keep the country safe and protect the freedoms that Americans hold dear. Our elected officials and those who are seeking office should embrace them with pride.
Endnotes


The bill provides an exception for suspect descriptions where there is “trustworthy information, relevant to the locality and timeframe, that links a person with a particular characteristic described in this paragraph to an identified criminal incident or scheme.” End Racial Profiling Act, H.R. 1498, 115th Cong. (2017), Sec. 2(7).

End Racial Profiling Act, H.R. 1498, 115th Cong. (2017), Sec. 2(8), 201(b)(4); End Racial and Religious Profiling Act of 2017 (ERRPA), S. 411, 115th Cong. (2017), Sec. 2(8), 201(b)(4).


ERRPA identifies two “covered programs” that trigger compliance: the Edward Byrne Memorial Justice Assistance Grant Program (“Byrne JAG” funding), and the “Cops on the Beat” program. End Racial Profiling Act of 2017, H.R. 1498, 115th Cong. (2017), Sec. 2(1); End Racial and Religious Profiling Act of 2017 (ERRPA), S. 411, 115th Cong. (2017), Sec. 2(1).


A bill to block the implementation of certain presidential actions that restrict individuals from certain countries from entering the United States, H.R. 4271, 115th Cong. (2017) (Chu); A bill to block the implementation of certain presidential actions that restrict individuals from certain countries from entering the United States, S. 1979, 115th Cong. (2017) (Murphy).


Ibid. at 247 (ECPA passed in 1986; the first web browser was not used until 1990).
See Electronic Communications Privacy Act, Title II, 18 U.S.C. § 2701 et seq. (Stored Communications Act) and Title III, 18 U.S.C. § 3121 et seq. (Pen Register Act).

See United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (reasoning that email “is the technological scion of tangible mail” and that it would “defy common sense to afford emails lesser Fourth Amendment protection”); In re Grand Jury Subpoena, JK-15-029, 828 F.3d 1083, 1091 (9th Cir. 2016) (finding a reasonable expectation of privacy in personal emails stored by a third-party service provider).


78 Ibid. at 1-11.