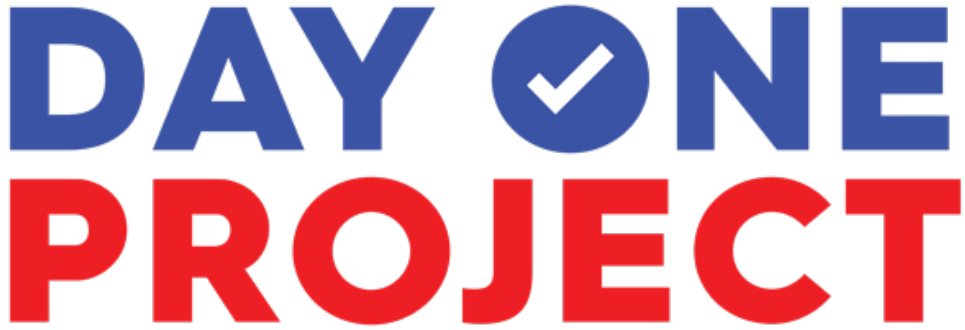

Mitigating Doxing Risks: Federal Strategies to Prevent Online Threats from Translating to Offline Harms

Michaela Lee
Kenny Chen

June 2021

The Day One Project offers a platform for ideas that represent a broad range of perspectives across S&T disciplines. The views and opinions expressed in this proposal are those of the author and do not reflect the views and opinions of the Day One Project or its S&T Leadership Council.

Summary

The Biden-Harris Administration should act to address and minimize the risks of malicious doxing,[1] given the rising frequency of online harassment inciting offline harms. This proposal recommends four parallel and mutually reinforcing strategies that can improve protections, enforcement, governance, and awareness around the issue.

The growing use of smartphones, social media, and other channels for finding and sharing information about people have made doxing increasingly widespread and dangerous in recent years. A 2020 survey by the Anti-Defamation League found that 44% of Americans reported experiencing online harassment.[2] 28% of Americans reported experiencing severe online harassment, which includes doxing as well as sexual harassment, stalking, physical threats, swatting,[3] and sustained harassment. In addition, a series of disturbing events in 2020 suggest that some instances of coordinated doxing efforts have reached a level of sophistication that poses a serious threat to U.S. national security. The pronounced spike in doxing cases against election officials,[4] federal judges,[5] and local government officials[6] should serve as evidence for the severity and urgency of this issue. Meanwhile, private citizens have faced elevated doxing risks as disruptions from the COVID-19 pandemic and tensions around contentious sociopolitical issues have provoked cycles of online harassment.[7]

While several states have proposed anti-doxing bills over the past year, most states do not offer adequate protections for doxing victims or mechanisms to hold perpetrators accountable. The doxing regulations that do exist are inconsistent across state lines, and partially applicable federal laws—such as the Interstate Communications Statute and the Interstate Stalking Statute—neither fully address the doxing problem nor are sufficiently enforced.[8] New federal legislation is a crucial step for ensuring that doxing risks and harms are appropriately addressed, and must come with complementary governance structures and enforcement capabilities in order to be effective.

[1] Doxing refers generally to publication of personally identifiable information with the intent to cause harm. A more detailed definition is provided in the FAQ of this proposal.
[2] Anti-Defamation League, *Online Hate and Harassment Report: The American Experience 2020*, 2020.
[3] Swatting is a form of harassment in which attackers try to trick police forces into sending a heavily armed strike force—often a SWAT team, which gives the technique its name—to a victim's home or business. Source: Josh Fruhlinger, "What is swatting? Unleashing armed police against your enemies." *CSO*, November 25, 2020.
[4] Ashley Nerbovig, "Wayne County canvassers doxxed and threatened over votes." *Detroit Free Press*, November 18, 2020.
[5] Nicole Hong, et. al., "Anti-Feminist Lawyer Is Suspect in Killing of Son of Federal Judge in N.J." *The New York Times*, July 20, 2020.
[6] Chad Mills, "After disruptive threats against city employees and others, Louisville leaders target 'doxing'." *WDRB*, March 4, 2021.
[7] Hannah Smothers, "Spring Breakers Viciously Defend Themselves Online After COVID-19 Outbreak." *Vice*, April 13, 2020.
[8] 18 U.S. Code § 875 - Interstate communications.

Challenge and Opportunity

Doxing is a pernicious tactic used to threaten, harass, silence, or endanger targets by sharing their personally identifiable information on the internet, typically with malicious intent. While the term has been used in some cases to describe activities legally protected by the First Amendment, the focus of this proposal is on malicious doxing, where actions online threaten to trigger real harms.

Such harms are myriad. Leaked addresses can lead to stalking and "swatting." Stolen bank account information can lead to hacked credit cards and fraudulent purchases. Compromised personal information can lead to extortion. It is important to recognize that a doxing incident does not need to result in a physical attack to cause harm. Doxing victims report experiencing severe mental and emotional duress, as well as suffering social and reputational damage when their information is accompanied with false statements or non-consensual intimate images.[9] 36% of those who are harassed online report stopping, reducing, or changing online behavior. 10% report moving houses, changing their commute, or avoiding places to protect themselves, indicating that these threats and their impacts are not contained to the online environment.[10]

Especially vulnerable and marginalized groups, such as women, minorities, and LGBTQ individuals, are disproportionately targeted by doxing threats. Doxers also frequently attack their targets' families, friends, and coworkers to cause additional harassment and intimidation. Doxing has become a common tactic used by hacktivists, disinformation networks, vengeful individuals, and, on occasion, the misled public as well. It is not uncommon for victims to be doxed by accident, through cases of mistaken identity or erroneous attribution of their online behavior.[11]

Doxing is likely to become even more widespread and harmful without intervention. Doxing attempts around political issues are increasing, and the practice is also starting to seep further into the private sector (e.g., irate employees targeting their former company or managers) and personal lives (e.g., vengeful super-spreaders of online smears) without significant repercussions.

Fortunately, an appetite for intervention exists. There is general consensus across social media platforms that doxing violates their rules, standards, and policies. Policy measures to address doxing have received bipartisan support in recent years. Both Democratic and Republican lawmakers have proposed state and federal legislation to criminalize doxing and provide protection to victims. U.S. House Democrats introduced the Interstate Doxxing Prevention Act (H.R.6478) in 2016,[12] while U.S. Senate Republicans introduced the Public Servant Protection Act

[9] Stine Eckert and Jade Metzger-Rifkin, "Doxing, Privacy and Gendered Harassment." *M&K Medien & Kommunikationswissenschaft*. 2020.
[10] Anti-Defamation League, *Online Hate and Harassment Report: The American Experience 2020*, 2020.
[11] Stine Eckert and Jade Metzger-Rifkin, "Doxing, Privacy and Gendered Harassment." 2020.
[12] Hamza Shaban, "Doxxing May Become A Federal Crime." *BuzzFeed News*, December 9, 2016.

(S.4965) in 2020.[13] State-level anti-doxing bills in Kentucky,[14] Oklahoma,[15] Oregon,[16] Nevada[17] have received largely bipartisan if not unanimous approval, albeit with varying approaches. There is also significant public support for further government action in this area. 87.5% of Americans report wanting stronger laws against online hate and harassment as well as better training and resources for law enforcement for responding to these threats.[18]

New federal legislation would provide legal clarity on what constitutes doxing, articulate the responsibilities of different parties when it comes to preventing and mitigating doxing, and ensure that protections for targets of doxing and severe online harassment are constitutional and comprehensive. Investments in training law enforcement and companies providing online services to recognize and address doxing are also needed. It is time for the U.S. government to act against online threats that result in real-world harms, lest these threats continue to escalate.

Plan of Action

There are multiple strategies that the Biden-Harris Administration can take to improve protections, enforcement, governance, and awareness around doxing. Below, we present a plan of action centered on four mutually reinforcing approaches: (1) legislative action, (2) expansion of enforcement capabilities, (3) establishment of a national task force, and (4) coordination of a national awareness campaign.

1. Pass legislation to criminalize malicious doxing and protect victims.

Appropriate anti-doxing legislation would (i) define and categorize doxing as a criminal act within Title 18 of the United States Code, and (ii) articulate processes for criminal and civil penalties and remedies to be pursued for perpetrators and victims of doxing, respectively. On December 8, 2016, Representative Katherine Clark (D-MA) introduced the Interstate Doxxing Prevention Act (H.R. 6478)—a general anti-doxing bill—to the 114th Congress.[19] The bill did not make it out of committee, but an updated version is scheduled to be introduced to the 117th Congress by Rep. Clark's office in 2021. On December 3, 2020, Senator Tom Cotton (R-AR) introduced the Public Servant Protection Act of 2020 (S. 4965)—a more specific bill for protecting government officials from doxing—to the 116th Congress.[20] The fact that anti-doxing proposals have come

[13] Tal Axelrod, "Republican senators introduce bill to protect government workers from being targeted at home." *The Hill*, December 3, 2020.
[14] Chad Mills, "Louisville leader applauds new state law that limits 'doxing'." *WDRB*, April 14, 2021.
[15] Kaylee Douglas, "Controversial anti-doxxing bill signed into Oklahoma law by Gov. Stitt." *KFOR*, April 21, 2021.
[16] Maxine Bernstein, "Oregon House passes package of police accountability measures." *The Oregonian*, April 26, 2021.
[17] John Sadler, "In move to quash online harassment, Nevada anti-doxxing bill advances. *Las Vegas Sun*, April 13.
[18] Anti-Defamation League, *Online Hate and Harassment Report: The American Experience 2020*, 2020.
[19] H.R. 6478 - Interstate Doxxing Prevention Act of 2016. 114th Congress.
[20] S. 4965 - Public Servant Protection Act of 2020. 116th Congress.

from both sides of the aisle signals an opportunity for bipartisan collaboration. Congress should prioritize moving these bills to the floor. As an alternative, key provisions from these bills could be incorporated into other legislation, such as the Violence Against Women Reauthorization Act, the SHIELD Act, the SAFE TECH Act, or other bills related to improving governance of criminal behavior online.

2. Issue a Presidential Memorandum directing law enforcement to (i) codify doxing in their data-reporting practices, and (ii) improve training and coordination around responses to online crimes.

Current law enforcement standards and data reporting processes do not include doxing as a category of incident that can be codified or reported on. As a result, the scope and severity of doxing has not been accurately quantified and remains insufficiently understood. Furthermore, because online crimes are not limited by physical borders, jurisdictional boundaries and responsibilities for managing doxing are unclear. Many local precincts do not have the resources or training to respond appropriately to online threats, especially when the source of a threat originates from outside of their jurisdiction.[21] On the other hand, doxing threats may often seem too small or insufficiently substantiated to warrant action from federal authorities. Because of the limited coordination between jurisdictions, responses to doxing threats are generally slow or ineffective, if addressed at all. To resolve these gaps, law enforcement agencies need to update systems and procedures so that online crimes and threats receive adequate reporting and responses from the appropriate jurisdictions. To aid this effort, President Biden should issue a Presidential Memorandum directing the Department of Justice and its component agencies, such as the FBI, to (i) review current procedures for (and gaps in) law enforcement responses to online crimes; (ii) develop model policies and best practices to aid state and local agencies in responding to doxing threats; and (iii) provide resources and support to help federal, state, and local agencies incorporate doxing into their reporting and training. The Memorandum should also direct the Office of the Director of National Intelligence (ODNI) to assume a central role in facilitating intelligence integration around cross-jurisdictional doxing threats.

3. Include doxing as a priority area in the Task Force on Online Harassment and Abuse.

Several provisions in the recent Violence Against Women Reauthorization Act of 2019 (VAWA 2019) articulate approaches to confronting online harassment, abuse, and stalking, behaviors that are closely related to doxing.[22] During his campaign, President Biden committed to convening a national Task Force on Online Harassment and Abuse, an entity that would be charged with developing strategies and recommendations for cross-sector stakeholders to

[21] Pen America, Online Harassment Field Manual. n.d.
[22] The Biden Plan to End Violence Against Women. Joebiden.com, 2020.

effectively prevent and respond to online threats. It is important that these efforts do not remain limited strictly to online harms, but also consider the risk of online activities translating to offline harms through actions like doxing. Whether or not VAWA 2019 is passed, the Biden-Harris Administration should fulfill its commitment to convening a Task Force on Online Harassment and Abuse responsible for providing guidance, oversight, and resources for relevant stakeholders. One specific duty that the Task Force should assume is developing and disseminating a set of toolkits that local law enforcement agencies, nonprofit organizations, employers, and private citizens could use to inform and coordinate responses to doxing threats.

4. Elevate national awareness and coordination around doxing risks.

The Biden-Harris Administration should work to raise public awareness of doxing (helping individuals and organizations understand the nature of the threat) and to align anti-doxing initiatives (helping individuals and organizations protect themselves). In particular, the Administration can instigate a public awareness campaign that informs people of their vulnerabilities in an online environment, highlights what steps they can take to protect themselves, and shares resources for commonly doxed groups and common doxing situations. We propose that this type of campaign should be spearheaded by the FBI and disseminated through their network of state, local, and civil society partners. It should also be undertaken in coordination with cross-sector stakeholders such as trade associations, news organizations, and social media platforms. Bipartisan cooperation in these actions is a real possibility. Though Democrats have emphasized the needs of vulnerable groups such as women, minorities, or LGBTQ communities, whereas Republicans have focused on protecting public servants such as police officers and elected officials, lawmakers from both parties have condemned doxing. The Biden-Harris Administration should be sure emphasize bipartisan messaging and engage leaders from both parties in elevating the importance of anti-doxing action.

Conclusion

Doxing stands at a dangerous nexus of online and offline harms. As the world becomes ever-more connected via internet technologies, smart devices, and services built on copious amounts of personal user data, the exposure and risks posed to private citizens and elected officials alike will continue to grow. Policymakers must rise to the challenge of confronting and mitigating the threat of doxing before its harms become more severe and widespread, or even threaten to cause irreparable damage to our society.

Frequently Asked Questions

How does this proposal define doxing?

In this proposal, we apply the definition of doxing articulated in H.R. 6478: "Publication of personally identifiable information with the intent to cause harm." H.R. 6478 further explains that doxing involves "the intent to threaten, intimidate, harass, stalk, or facilitate another to threaten, intimidate, harass, or stalk, uses the mail or any facility or means of interstate or foreign commerce to knowingly publish the personally identifiable information of another person, and as a result of that publication places that person in reasonable fear of the death of or serious bodily injury to—(1) that person; (2) an immediate family member of that person; or (3) an intimate partner of that person."

How do proposed anti-doxing measures threaten or uphold First Amendment protections for freedom of speech?

Under the First Amendment, doxing could be considered protected speech unless it crosses the line into incitement to imminent lawless action or true threats.

The Interstate Stalking Statute (18 U.S.C. Section 2261A), initially enacted as part of the Violence Against Women Act, prohibits cyberstalking. Specifically, the legislation criminalizes use of the mail or "any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to [a] person or places that person in reasonable fear of the death of, or serious bodily injury to" the person.

Thus far, federal courts have rejected First Amendment challenges to the Interstate Stalking Statute in United States v. Bowker (6th Cir. 2004; reversed on other grounds) and United States v. Shrader (U.S. Dist. W.V. 2010).

In fact, limiting doxing may actually help further the goals of the First Amendment. As Mary Anne Franks of Columbia University has pointed out, doxing chills free speech by causing "psychological effects — lack of confidence, social anxiety, fear — but also physiological effects, such as increased heart rate and stress. This in turn can lead to targets censoring themselves as a means of avoiding these negative effects."[23]

[23] Mary Anne Franks, "The Free Speech Black Hole: Can The Internet Escape the Gravitational Pull of the First Amendment?" Knight First Amendment Institute at Columbia University, August 21, 2019.

How prevalent is doxing?

Unfortunately, because of inconsistencies in reporting and codifying doxing incidents, it is impossible to precisely measure the full scale and impact of doxing. However, research that has been done reveals deeply concerning trends. The Anti-Defamation League's 2020 report on online hate and harassment found that 44% of Americans had experienced some form of online harassment, 15% had received physical threats, and 12% had experienced stalking.[24] A 2017 paper presented an analysis of 1.7 million text files posted to pastebin.com, 4chan.org, and 8ch.net (common sites for sharing doxes) over the course of 13 weeks, and found over 4,000 instances of doxing.[25] Better understanding of the prevalence of doxing requires improved capture and reporting of relevant data, especially from law enforcement.

How is doxing currently addressed under law?

There are three federal statutes that partially, but insufficiently, address doxing: Section 230 of the Communications Decency Act (CDA); the Interstate Communications Statute (18 U.S.C. Section 875(c)); and the Interstate Stalking Statute (18 U.S.C. Section 2261A). Additionally, most states have criminalized cyberstalking or have applied criminal harassment statutes to online activity, to different degrees of strength. Unfortunately, neither federal nor state laws sufficiently protect victims from doxing. Many laws specify that in order to be considered a crime, doxing must be accompanied by an additional, specific threat of violence. Enforcement of relevant statutes in doxing cases is also extremely low. Many law enforcement officers are unaware that these statutes can be used in doxing cases, and there are few resources to help law enforcement investigate and prosecute doxing cases.

Is new legislation needed to address doxing? Aren't there other ways to tackle the issue?

New legislation is necessary to address present gaps in protections and accountability mechanisms around doxing. However, it is also clear that doxing occupies a complex area of cyber rights and crimes that remains insufficiently understood, regulated, and codified. As such, in addition to legislative action, we recommend complementary executive and judicial strategies that would provide additional resources, clarity, and attention around doxing issues.

---

[24] Anti-Defamation League, *Online Hate and Harassment Report: The American Experience 2020*, 2020.

[25] Peter Snyder, et al., "Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing," *Proceedings of IMC '17*. ACM, New York, NY, 2017.

About the Authors

Michaela Lee works at the intersection of emerging technology, policy, and human rights. She is currently pursuing a Master's in Public Policy degree at the Harvard Kennedy School and is a Research Assistant with the Belfer Center, focused on cyber, emerging tech, and international security. Prior to joining the Kennedy School, Michaela served as a Tech and Human Rights Manager at BSR, where she covered responsible AI, end-to-end encryption, disinformation and hate speech, and platform governance. She was an Assembly Fellow on disinformation with the Berkman Klein Center for Internet & Society at Harvard and a Coro Fellow in Public Affairs.

Kenny Chen is a Master's student in Public Policy at the Harvard Kennedy School, and a researcher at Harvard's Technology and Public Purpose Project. He applies a cross-sector and multidisciplinary background toward exploring concepts of trust and trustworthiness in human-AI systems. Previously, Kenny served as Co-Founder and Executive Director of the Partnership to Advance Responsible Technology (PART) and PGH.AI. He remains an active member of various international communities and initiatives around AI ethics, policy, and governance, including XPRIZE, AI Commons, and the UN's AI for Good platform.

About the Day One Project

The Day One Project is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community to develop actionable policies that can improve the lives of all Americans. For more about the Day One Project, visit dayoneproject.org