

U.S. ASYLUM LAW AND THE DIGITAL INFORMATION ENVIRONMENT

*Liane M. Jarvis Cooper**

ABSTRACT

In this new era of digital dissidents and digital persecutors, targeted individuals and groups will flee their home countries, seeking protection in the United States. U.S. federal courts and agencies will thus need to develop coherent judicial, regulatory, and policy frameworks to address asylum claims involving the digital information environment. This essay uncovers and analyzes key issues that the U.S. asylum system must consider when formulating frameworks to address such claims.

* J.D., University of Michigan Law School, 2001; A.B., Occidental College, 1998. The author has served as an Asylum Officer with the U.S. Department of Homeland Security and in several attorney positions with the U.S. Department of Justice, including as Chief Regulatory Counsel and Associate General Counsel in the Executive Office for Immigration Review's Office of the General Counsel. The views in this essay are solely the author's and do not reflect those of any employers. The author would like to thank Ellen Liebowitz and the editors of the Houston Journal of International Law, including Julia M. Tape, Anu Reddy, and Bailey Pruitt.

ABSTRACT	45
INTRODUCTION	46
II. SETTING THE VIRTUAL STAGE	48
III. KEY ISSUES.....	53
A. Coexistence of Online and Offline Harms.....	54
B. Presence of Past and Future Harms	55
C. Emergence of Transnational Persecution	56
D. Emergence of Novel Harms	60
E. Unique and Disproportionate Targeting.....	62
F. Increased Significance of Non-State Actors	64
G. Evidentiary Concerns.....	67
H. Caseload and Fraud Concerns	69
IV. CONCLUSION	70

INTRODUCTION

Imagine Kate. She has boarded an airplane and fled her home country. After arriving in the United States, she checks into a hostel and barricades herself in her room. She is frightened. Her government back home has shut down her blog criticizing the regime. Compatriot dissidents have been arrested. She turns on her smartphone and launches Twitter. She tweets:

I need political asylum.

This is the new era of digital dissent. Online, dissidents and marginalized individuals share their opinions, beliefs, and identities; articulate their fears of future persecution; and ask for help in real time.¹ This is also the era of savvy persecutors who

1. See, e.g., Richard C. Paddock & Ben Hubbard, *Saudi Woman Who Tried to Flee Family Says, 'They Will Kill Me'*, N.Y. TIMES (Jan. 6, 2019), <https://www.nytimes.com/2019/01/06/world/middleeast/saudi-thailand-rahaf-alqunun.html> [<https://perma.cc/ZCG4-57FW>]; *Rahaf al-Qunun: Saudi Woman Ends Airport Hotel Standoff*, BBC NEWS (Jan. 7,

engage in online measures to stifle dissent and target dissidents and marginalized groups.² Some targeted individuals will consequently flee their home countries, seeking asylum in the United States.³ Their experiences in the digital information environment and at the receiving end of technology-assisted threats and harm will provide evidence of past and future persecution.⁴ The U.S. asylum system must develop coherent judicial, regulatory, and policy frameworks to address these digital dissidents' requests for asylum.

This essay uncovers and analyzes key issues that U.S. federal courts and agencies will encounter when formulating frameworks to address asylum claims involving the digital information environment. This essay proceeds as follows. To appreciate how these claims may arise, Part II provides background on how and why persecutors, dissidents, and marginalized individuals participate in and are affected by the digital information environment. Part III then examines eight issues that the U.S. asylum law system must consider as it develops frameworks to address these claims.

2019), <https://www.bbc.com/news/world-middle-east-46777848> [<https://perma.cc/DWD2-S5D2>].

2. See Dorota Głowacka et al. (European Parliament Directorate-Gen. for External Pol'ys), *Digital Technologies as a Means of Repression and Social Control*, at 14–32 (Apr. 2021), [https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU\(2021\)653636](https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653636) [<https://www.doi.org/10.2861/6706>].

3. See, e.g., Mark Trevelyan, *Russian Whose Daughter Drew Anti-War Picture Gets Two Years' Jail But Flees*, REUTERS (Mar. 28, 2023), <https://www.reuters.com/world/europe/russian-father-whose-daughter-drew-anti-war-picture-given-two-years-jail-2023-03-28/> [<https://web.archive.org/web/20230328130557/https://www.reuters.com/world/europe/russian-father-whose-daughter-drew-anti-war-picture-given-two-years-jail-2023-03-28/>]; Valerie Hopkins, *She Posted Online About the War in Ukraine. Then She Faced a Prison Term.*, N.Y. TIMES (Mar. 22, 2023), <https://www.nytimes.com/2023/03/22/world/europe/russia-ukraine-social-media-crackdown.html> [<https://web.archive.org/web/20230322093757/https://www.nytimes.com/2023/03/22/world/europe/russia-ukraine-social-media-crackdown.html>].

4. See, e.g., *Flores Molina v. Garland*, 37 F.4th 626, 630–40 (9th Cir. 2022) (finding past persecution where an asylum-seeker was forced to flee his home country after being threatened online and offline and remanding to the agency to reconsider whether the asylum-seeker has a well-founded fear of future persecution).

II. SETTING THE VIRTUAL STAGE

The digital information environment serves many purposes for dissidents and marginalized individuals. While it exists for some as an echo-chamber reinforcing their pre-existing beliefs,⁵ it may function for others as a foundry for identity-experimentation, -formation, and -expression.⁶ In the digital information environment, individuals may be exposed to a variety of people and ideas, allowing them to cultivate new relationships, identities, and communities, as well as strengthen pre-existing ones.⁷

Crucially, the digital information environment provides dissidents and marginalized individuals with a platform to share their beliefs and express their political, national, religious, racial, social, cultural, gender, and sexual identities. On social media, for instance, political dissidents can spread their opinions to wide and varied audiences, reaching across national borders, languages, and cultures. Journalists and ordinary individuals can act as digital witnesses and advocates, recording human rights violations on smartphones and campaigning on social media for transnational solidarity and accountability.⁸ Targeted

5. See Matteo Cinelli et al., *Echo Chambers on Social Media: A Comparative Analysis* 4–6 (Apr. 20, 2020), <https://arxiv.org/abs/2004.09603> [<https://doi.org/10.48550/arXiv.2004.09603>]; Walter Quattrociocchi, *Inside the Echo Chamber*, SCIENTIFIC AM., Apr. 2017, at 60–63, republished online as *Why Social Media Became the Perfect Incubator for Hoaxes and Misinformation* (Apr. 1, 2017), <https://dx.doi.org/10.1038/scientificamerican.0417-60>.

6. See Anas Ansar & Abu Faisal Md. Khaled, *In Search of a Rohingya Digital Diaspora: Virtual Togetherness, Collective Identities and Political Mobilization*, 10(61) HUMAN. SOC. SCI. COMMUN. 4–10 (2023); Abdul Aziz, *Rohingya Diaspora Online: Mapping the Spaces of Visibility, Resistance and Transnational Identity on Social Media*, NEW MEDIA & SOC'Y 9–17 (2022).

7. See Jay M. Marlowe et al., *Digital Belongings: The Intersections of Social Cohesion, Connectivity and Digital Media*, 17 ETHNICITIES 2, 7–14 (2017); Sara Marino, *Making Space, Making Place: Digital Togetherness and the Redefinition of Migrant Identities Online*, 1(2) SOCIAL MEDIA + SOC'Y 6 (2015).

8. See Adrian Shahbaz et al., *FREEDOM ON THE NET 2022: COUNTERING AN AUTHORITARIAN OVERHAUL OF THE INTERNET* 3, 12 (Freedom House, Oct. 2022); Marie Gillespie et al., *MAPPING REFUGEE MEDIA JOURNEYS: SMARTPHONES AND SOCIAL MEDIA NETWORKS* 25–26 (The Open University/France Medias Monde, 2016); Sam Gregory, *Ubiquitous Witnesses: Who Creates the Evidence and the Live(d) Experience of Human Rights Violations?*, 18 INFO., COMM'N & SOC'Y 1378–92 (2015); see, e.g., Human Rights

individuals can also document and communicate in the digital realm their personal experiences of past harm and fears of future harm.⁹ Even third parties may assist in digitally recording and broadcasting on behalf of those targeted.¹⁰ For those fleeing persecution, the digital information environment also provides a necessary channel for coordinating migration routes; learning about the destination country, including its culture and language; connecting with communities in the diaspora; and obtaining information about family members and events in their home countries.¹¹ When traditional media and historical modes of communication are lacking or fail, the digital information environment may function as the principal—or, even, the only—medium of expression, communication, and protest.¹²

Like dissidents and marginalized individuals, governments and non-state bad actors also actively respond to and participate in the digital information environment.¹³ Authoritarian regimes use legislation and the legal system to restrict and forbid online dissent.¹⁴ They detain, arrest, and prosecute individuals for their

Watch, WORLD REPORT 2023: EVENTS OF 2022 56, 152–53, 155–56, 176, 355–56, 406, 507, 519, 621, 678 (2023); Amnesty Int'l, ANNUAL WORLD REPORT 2022/23 194, 401–02 (2023).

9. See, e.g., Rahaf Mohammed (@rahaf84427714), TWITTER (Jan. 5, 2019, 9:21 PM), <https://web.archive.org/web/20200127141958/https://twitter.com/rahaf84427714/status/1081782663344807937>; Rahaf Mohammed (@rahaf84427714), TWITTER (Jan. 6, 2019, 12:04 PM), <https://web.archive.org/web/20190106203339/https://twitter.com/rahaf84427714/status/108200512101632000>. To read Ms. Mohammed's account of her experience, see generally Rahaf Mohammed, REBEL: MY ESCAPE FROM SAUDI ARABIA TO FREEDOM (Harper Collins Canada, 2022).

10. See, e.g., Kayleen Devlin, *Flying Without a Man: The Mysterious Case of Dina Ali*, BBC NEWS (Jun. 1, 2017), <https://www.bbc.com/news/blogs-trending-40105983> [<https://perma.cc/A8JN-6TGU>].

11. See Gillespie et al., *supra* note 8, at 50; Maren Borkert et al., *The Best, the Worst, and the Hardest to Find: How People, Mobiles, and Social Media Connect Migrants in(to) Europe*, 4(1) SOCIAL MEDIA + SOC'Y 6 (2018); Mark Latonero & Paula Kift, *On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control*, 4(1) SOCIAL MEDIA + SOC'Y 1, 3–4 (2018).

12. See, e.g., Human Rights Watch, *supra* note 8, at 153, 606.

13. See, e.g., U.N. Office of the High Commissioner for Human Rights, Human Rights Impacts of New Technologies on Civic Space in South-East Asia 4–7 (May 30, 2023), <https://www.ohchr.org/sites/default/files/documents/issues/civicspace/OHCHR-TECHCS-SEA2023.pdf> [hereinafter OHCHR].

14. See, e.g., Human Rights Watch, *supra* note 8, at 56–57, 69, 113, 421, 423, 446, 487–88, 498, 502–03, 519, 529, 553, 590, 593, 604, 606–07, 619, 625, 647, 678; Amnesty Int'l, *supra* note 8, at 85, 93, 194, 369, 382–83, 401–02.

online content, communications, and activities.¹⁵ In addition to outright restrictions on digital dissent, they also foment a precarious digital information environment by arbitrarily allowing some instances of online presence while disallowing others.¹⁶ And, critically, both state and non-state actors threaten and engage in physical violence against digital dissidents.¹⁷

Authoritarian regimes and non-state bad actors also employ a host of evolving technologies to disrupt and suppress dissidents and marginalized individuals' online presences and communication, thereby drowning out dissent. Governments implement measures such as digital surveillance and censorship; disinformation campaigns and online manipulation; flooding of state content; coordinated hacking attacks, social media dogpiling, and digital threats; disruptions in internet connectivity and access; and outright internet shutdowns.¹⁸ As researchers Adrian Shahbaz et al. have explained, governments also digitally fence in individuals by restricting the flow of news and information, asserting state control over internet infrastructure, and erecting barriers to cross-border transfers of user data.¹⁹ Simultaneously, governments reach beyond national and physical borders to target dissidents in diaspora communities through online surveillance and other digital measures.²⁰

15. See, e.g., Human Rights Watch, *supra* note 8, at 21–22, 25, 56–57, 152, 155–56, 215, 292, 349, 355–56, 394, 406, 420, 423, 487–88, 502–03, 507, 519, 530, 586–87, 606–07, 620–21, 647, 678; Amnesty Int'l, *supra* note 8, at 85, 93, 194, 309, 362, 369, 376, 383, 401–02.

16. See Aysenur Dal et al., *Signaling Silence: Affective and Cognitive Responses to Risks of Online Activism About Corruption in an Authoritarian Context*, 25 NEW MEDIA & SOC'Y 646, 646–47 (2023); see also Rebecca MacKinnon, *Liberation Technology: China's "Networked Authoritarianism,"* 22(2) J. DEMOCRACY 32, 33 (2011); see, e.g., Human Rights Watch, *supra* note 8, at 153, 155–56, 176, 311, 349, 421, 501–02, 560, 586, 606–07, 619–20, 643, 646–47; Amnesty Int'l, *supra* note 8, at 194–95, 309, 362.

17. See, e.g., Human Rights Watch, *supra* note 8, at 21–22, 25, 56–57, 486, 507; Amnesty Int'l, *supra* note 8, at 156, 194, 376, 402 n.4.

18. See, e.g., Human Rights Watch, *supra* note 8, at 65, 113, 152–53, 155–56, 176, 196, 261–62, 311, 349, 421, 423, 445, 501–02, 519, 530, 560, 586, 619–20, 646–47, 679, 706; Amnesty Int'l, *supra* note 8, at 156, 194–95, 253, 362, 369.

19. Shahbaz et al., *supra* note 8, at 2–3; see, e.g., Human Rights Watch, *supra* note 8, at 511, 619–21.

20. See Yana Gorokhovskaia et al., *STILL NOT SAFE: TRANSNATIONAL REPRESSION IN 2022* 1, 4 (Freedom House, Mar. 2023).

Those targeted are a diverse population. They are journalists, writers, and bloggers. Even programmers and engineers, whose work protects and enhances digital expression and privacy, may be attacked online and offline. Regardless of background and prior experience in the digital information environment, these targeted individuals espouse or support others who hold opinions, beliefs, and identities that authoritarian regimes and non-state bad actors seek to suppress.²¹

Governmental and non-state measures to disrupt online dissent are harmful. Such measures can lead to offline, physical violence.²² Targeted individuals also lose their ability to participate in online spaces free from attack.²³ As a result, targeted individuals may be emotionally traumatized; lose their confidence and autonomy; feel stigmatized and dehumanized; experience profound and long-lasting fear and shame; suffer professional, reputational, and economic injuries; and experience damage to their relationships.²⁴ Some dissidents and targeted individuals may conceal their identities, self-censor, or reduce their presence in the digital realm.²⁵ Others may conform their

21. See, e.g., *Offline: Imprisoned Bloggers and Technologists*, ELEC. FRONTIER FOUND., <https://www.eff.org/offline> [<https://perma.cc/9AXQ-DJMA>] (last visited Jun. 11, 2023); Human Rights Watch, *supra* note 8, at 530, 619–21; see also Haifeng Huang v. Garland, 851 F. App'x 38, 39–40, n.2 (9th Cir. 2021).

22. See, e.g., Amnesty Int'l, *THE SOCIAL ATROCITY: META AND THE RIGHT TO REMEDY FOR THE ROHINGYA*, at 32–34 (2022) [hereinafter Amnesty Int'l, *THE SOCIAL ATROCITY*].

23. Cf. Emily Laidlaw, *Online Shaming and the Right to Privacy*, 6(3) LAWS 1, 10, 18 (2017) (theorizing that online shame produces this harm).

24. See Irene Khan (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶23, U.N. Doc. A/76/258 (Jul. 30, 2021); see, e.g., Amnesty Int'l, *THE SOCIAL ATROCITY*, *supra* note 22, at 32–34; cf. Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 BOS. UNIV. L. REV. 793, 831, 834–38, 840–50, 853–56, 859–61 (2022) (theorizing that online and offline privacy violations produce these harms).

25. See Dal et al., *supra* note 16, at 658; see, e.g., Allie Funk et al., *China*, in FREEDOM ON THE NET 2023 (Freedom House, Oct. 2023), <https://freedomhouse.org/country/china/freedom-net/2023> [<https://perma.cc/Z6CH-YJQH>]; Marilyn Clark & Anna Grech, *JOURNALISTS UNDER PRESSURE: UNWARRANTED INTERFERENCE, FEAR & SELF-CENSORSHIP IN EUROPE 14* (Council of Europe, 2017), <https://rm.coe.int/168070ad5d>; Gillespie, *supra* note 8, at 76–77; see also Sam Gregory, *Technology and Citizen Witnessing: Navigating the Friction Between Dual Desires for Visibility and Obscurity*, 26 THE FIBRECULTURE J. 268, 268–69 (2015).

online and offline speech, conduct, or behavior to perceived social norms.²⁶ Still others may leave the internet entirely.²⁷ Some will even flee their home countries,²⁸ seeking protection as asylum-seekers and refugees. Even post-flight, targeted individuals may disconnect and refrain from media usage to avoid further dangers to themselves and others back home.²⁹

Significantly, governmental and non-state bad actors' measures in the digital information environment not only chill dissidents' self-expression but also obstruct the free flow of communication and ideas that is essential for healthy, democratic discourse.³⁰ Such digital measures may implicate and infringe upon rights and freedoms protected under international law, including the freedom of expression; freedom of religion; the right to privacy; and the right to seek, receive, and impart information.³¹ In other words, due to such measures, dissidents and marginalized individuals are thwarted in their ability to engage in the conduct that is necessary for the exercise of their human rights. Actual and attempted restrictions in the digital information environment on individuals' opinions, beliefs, and identities may even be tantamount to persecution under U.S.

26. See Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1454–55, 1458 (2022); see also Liane M. Jarvis Cooper, *Sexual Privacy and Persecution*, 70 UCLA L. REV. DISC. 112, 117 (2022) [hereinafter Jarvis Cooper, *Sexual Privacy & Persecution*].

27. See Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 116; cf. Yana Gorokhovskaia & Isabel Linzer, DEFENDING DEMOCRACY IN EXILE: POLICY RESPONSES TO TRANSNATIONAL REPRESSION 27 (Freedom House, Jun. 2022) [hereinafter Gorokhovskaia & Linzer, POLICY RESPONSES] (discussing this effect in the context of transnational digital targeting of dissidents in the diaspora and exile communities).

28. See, e.g., Human Rights Watch, *supra* note 8, at 604.

29. See, e.g., *id.* at 507, 587; NATE SCHENKKAN & ISABEL LINZER, OUT OF SIGHT, NOT OUT OF REACH: THE GLOBAL SCALE AND SCOPE OF TRANSNATIONAL REPRESSION 13–14 (Freedom House, Feb. 2021); Stephanie Yang & David Shen, *These Friends Don't Know One Another's Real Name. Why? It's Too Dangerous*, L.A. TIMES (Apr. 6, 2023), <https://www.latimes.com/world-nation/story/2023-04-06/china-protesters-boston-keep-identities-hidden> [<https://perma.cc/H26R-ZDC8>].

30. See Khan, *supra* note 24, ¶23.

31. See G.A. Res. 217 (III) A, Universal Declaration of Human Rights, arts. 12, 18, 19 (Dec. 10, 1948); see also Yana Gorokhovskaia & Isabel Linzer, *Unsafe in America: Transnational Repression in the United States*, in DEFENDING DEMOCRACY IN EXILE: POLICY RESPONSES TO TRANSNATIONAL REPRESSION 4–5 (Freedom House, Jun. 2022).

asylum law.³² And, unfortunately, as digital technologies further evolve, the potential scale and scope of harm to dissidents and marginalized individuals may increase.³³ Thus, it is imperative that the U.S. asylum system develops legal frameworks to address conduct and harm attributable to the digital information environment.

III. KEY ISSUES

In addressing asylum claims involving the digital information environment, the crucial legal question will be whether and under which circumstances conduct, harms, threats, and events attributable to that environment are evidence of a well-founded fear of future persecution. To establish a well-founded fear of future persecution under U.S. asylum law, asylum-seekers must present evidence that they fear being persecuted on account of their race, religion, nationality, membership in a particular social group, or political opinion.³⁴ As illustrated in Figure 1, there are at least eight issues that the U.S. asylum system must consider when formulating frameworks to address such claims involving the digital information environment.

32. Cf. *Aden v. Wilkinson*, 989 F.3d 1073, 1083 (9th Cir. 2021) (explaining in the offline context that to make a persecution determination, “[a]nother important consideration is whether the threat leaves the person with no realistic choice but to conform to the persecutor’s way of life and forsake other political or religious beliefs, or flee”); *Kantoni v. Gonzales*, 461 F.3d 894, 898 (7th Cir. 2006) (“A credible threat that causes a person to abandon lawful political or religious associations or beliefs is persecution.”); *Krotova v. Gonzales*, 416 F.3d 1080, 1086–87 (9th Cir. 2005) (finding cumulative past persecution, in part, where the targeted individual was restricted in her ability to practice her religion); *Bucur v. INS*, 109 F.3d 399, 405 (7th Cir. 1997) (“[I]t is virtually the definition of religious persecution that the votaries of a religion are forbidden to practice it.”); see also *Mamouzian v. Ashcroft*, 390 F.3d 1129, 1137 n.6 (9th Cir. 2004) (noting that an individual is not required to renunciate her political beliefs to avoid future persecution).

33. See, e.g., Vivek Nair et al., *Exploring the Privacy Risks of Adversarial VR Game Design*, in PROC. 23RD PRIVACY ENHANCING TECHNOLOGIES SYMP. 238 (2023), <https://doi.org/10.56553/popets-2023-0108> (presenting a case study of how metaverse environments can be constructed to infer data covertly from seemingly anonymous users).

34. See 8 U.S.C. §§ 1101(a)(42)(A), 1158 (2023); 8 C.F.R. §§ 208.13(a), 1208.13(a) (2023); *INS v. Elias-Zacarias*, 502 U.S. 478, 481–82 (1992).

Figure 1—Issues to Consider in Addressing Asylum Claims Involving the Digital Information Environment.

1	Coexistence of Online & Offline Harms	5	Unique & Disproportionate Targeting
2	Presence of Past & Future Harms	6	Increased Significance of Non-State Actors
3	Emergence of Transnational Persecution	7	Evidentiary Concerns
4	Emergence of Novel Harms	8	Caseload & Fraud Concerns

A. Coexistence of Online and Offline Harms

Asylum claims involving the digital information environment and accompanying technologies are likely to involve a mix of online and offline conduct, harms, threats, events, and technologies. From a practical standpoint for adjudicating asylum claims, as well as developing agency regulations and policies, this means recognizing that dissidents and marginalized individuals’ lives and experiences may occur online and offline. Similarly, persecutors may also operate online and offline.

Let us return to the hypothetical at the beginning of this essay to illustrate the coexistence of online and offline harms. Assume that Kate is in the United States and applies for asylum, alleging that she fears being persecuted in the future by her home country’s government on account of her political opinion. To support her asylum claim, she may present evidence that her home country surveilled her online in response to her online and offline communications and activities. She may also testify that, due to her blog, she fears being detained, arrested, or physically harmed if she were to return to her home country. All such evidence may be relevant to establishing a well-founded fear of future persecution.³⁵

35. See Liane M. Jarvis Cooper, *Social Media and Online Persecution*, 35 GEO. IMMIGR. L.J. 749, 772–73 (2021) [hereinafter Jarvis Cooper, *Social Media & Online Persecution*]; see generally 8 U.S.C. §§ 1158(b)(1)(B)(i)–(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a) (delineating an asylum-seeker’s burden in establishing asylum eligibility).

B. Presence of Past and Future Harms

Asylum claims dealing with the digital information environment may also involve allegations of past and future harm. To establish that their fear of future persecution is well-founded, asylum-seekers must present evidence that the likelihood of future persecution is objectively reasonable.³⁶ Asylum-seekers must additionally demonstrate that their fear of future persecution is subjectively genuine.³⁷ Individuals who have experienced past persecution are presumed to have a well-founded fear of future persecution. Individuals who have not experienced past persecution or fail to establish a claim of past persecution must prove independently that their fear of future persecution is well-founded.³⁸

With respect to asylum claims involving the digital information environment, this means showing that conduct, harms, threats, and events attributable to that environment are evidence of past or future persecution.³⁹ For instance, returning to Kate, let us assume that she was surveilled on social media in her home country and testifies that the surveillance was due to her participation in online and offline protest movements. That online surveillance may be evidence of past persecution, triggering a presumption of future persecution.⁴⁰ Alternatively, in

36. See *INS v. Cardoza-Fonseca*, 480 U.S. 421, 430–31 (1987).

37. See *id.*; see also *Parada v. Sessions*, 902 F.3d 901, 909 (9th Cir. 2018).

38. See 8 C.F.R. §§ 208.13(b)(1), 1208.13(b)(1). Under some circumstances, individuals who have been persecuted in the past but no longer fear future persecution may be granted relief on humanitarian grounds. See 8 C.F.R. §§ 208.13(b)(1)(iii), 1208.13(b)(1)(iii).

39. See generally 8 U.S.C. §§ 1158(b)(1)(B)(i)–(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a) (delineating an asylum-seeker's burden in establishing asylum eligibility).

40. Cf. *Aden v. Wilkinson*, 989 F.3d 1073, 1083–84 (9th Cir. 2021) (holding that offline monitoring supports a finding of past persecution); *Manzur v. U.S. Dep't of Homeland Sec.*, 494 F.3d 281, 292–93 (2d Cir. 2007) (similar); see also *Ayele v. Holder*, 564 F.3d 862, 871 (7th Cir. 2009) (noting that surveillance “has been recognized as a possible form of persecution” in the Seventh Circuit); *Begzatowski v. INS*, 278 F.3d 665, 669 (7th Cir. 2002) (noting that “[t]ypes of actions that might cross the line from harassment to persecution include . . . surveillance”) (citation omitted); but see *Kazemzadeh v. U.S. Att'y Gen.*, 577 F.3d 1341, 1353 (11th Cir. 2009) (finding that the asylum-seeker had not been persecuted even though, among other harms, he was monitored offline); *Zheng v. U.S. Att'y Gen.*, 451 F.3d 1287, 1291 (11th Cir. 2006) (similar); *Roman v. INS*, 233 F.3d 1027, 1034 (7th Cir. 2000) (similar).

the absence of an agency or court's finding that past persecution has occurred, the past online surveillance may be evidence that Kate's government is likely to persecute her in the future.⁴¹ As another example, consider the scenario in which government officials publish posts on Facebook threatening Kate and her fellow dissidents. Those social media posts may serve as evidence of both past and future persecution.⁴²

C. Emergence of Transnational Persecution

This is the epoch of transnational persecution. In this new era, conduct, harms, threats, and events in the digital information environment seemingly defy time and physical boundaries.⁴³ These time-defying and transnational aspects of the digital information environment are likely to challenge—but are not incompatible with—the United States' current, legal conceptualizations of the temporal and physical boundaries of persecution. Under current U.S. regulations, only harm that occurred in an asylum-seeker's home country or country of last habitual residence may be considered past persecution.⁴⁴ Digital harm originating from and directed at an asylum-seeker while she was still physically within her home country would readily meet this regulatory requirement. For instance, being threatened on social media by government officials while still within one's

41. Cf. *Zhang v. Ashcroft*, 388 F.3d 713, 717–18 (9th Cir. 2004) (finding that past, offline monitoring of the asylum-seeker's parents supports his request for the relief of withholding of removal); *Nasseri v. Moschorak*, 34 F.3d 723, 729 (9th Cir. 1994) (finding that past, offline surveillance of the asylum-seeker supports her request for the relief of withholding of deportation); see generally 8 U.S.C. § 1231; 8 C.F.R. §§ 208.16, 1208.16 (governing the relief of withholding of removal which differs from the relief of asylum).

42. See, e.g., *Flores Molina*, 37 F.4th at 630–37 (providing three bases to find past persecution where an asylum-seeker was threatened online and offline and remanding to the agency to reconsider whether the asylum-seeker has a well-founded fear of future persecution); see also *Espinoza v. U.S. Att'y Gen.*, no. 23–1453, at 6 n.6 (3rd Cir., Dec. 1, 2023) (non-precedential) (noting that the agency observed that social media threats may be relevant to establishing a well-founded fear of future persecution but denying on other grounds).

43. See Gorokhovskaia & Linzer, *POLICY RESPONSES*, *supra* note 27, at 1–2, 8, 15, 26–32; Schenkkan & Linzer, *supra* note 29, at 2, 4–6, 13–15, 18, 22, 25, 29, 35, 44–46, 48, 50.

44. See 8 C.F.R. §§ 208.13(b)(1), 1208.13(b)(1).

country's national borders should be considered relevant in assessing whether past persecution has occurred.⁴⁵

For past persecution claims, the more challenging aspect is recognizing that targeted individuals may also experience digital conduct and harm as ongoing and seemingly inescapable despite the passage of time or crossing of physical borders. There are two points to be made here. The first is that, while the initiation of the online conduct and harm may be in the targeted individual's home country, the locus of the conduct and its resulting injuries may be transported and continue abroad. Threatening tweets do not disappear when one relocates physically. The second point is that the unique aspects of the digital information environment, including the potential for online conduct and harm to be repetitive, permanent, searchable, and disseminated to wide and varied audiences, may increase the magnitude of the asylum-seekers' injuries regardless of when and where the harmful online conduct began.

For instance, an attack on social media that originated in and was initially directed at Kate while she was still in her home country may cause her profound emotional trauma even post-flight. Her emotional injury may be further compounded by the amplifying nature of the online realm in which harmful content easily propagates and mutates despite efforts to quash it.⁴⁶ In such a scenario, Kate's emotional trauma may alone or in conjunction with other conduct, harms, threats, and events amount to past persecution.⁴⁷

45. See Jarvis Cooper, *Social Media & Online Persecution*, *supra* note 35, at 780–81.

46. See Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 134; *see, e.g.*, Amnesty Int'l, *THE SOCIAL ATROCITY*, *supra* note 22, at 38–49 (discussing the various ways that harmful content propagates on Facebook and consequently fuels offline violence); *cf.* Gorokhovskaia & Linzer, *POLICY RESPONSES*, *supra* note 27, at 27–29, 31–32 (detailing dissidents' precautions against digital transnational repression, as well as their logistical and emotional difficulties in seeking redress from social media platforms).

47. See Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 128–29, 134; Jarvis Cooper, *Social Media & Online Persecution*, *supra* note 35, at 752, 773–78; *see generally* Makhoul v. Ashcroft, 387 F.3d 75, 80 (1st Cir. 2004) (acknowledging, in the offline context, that “under the right set of circumstances, a finding of past persecution might rest on a showing of psychological harm”) (citations omitted); *Mashiri v. Ashcroft*, 383 F.3d 1112, 1120 (9th Cir. 2004) (“Persecution may be emotional or psychological, as well as physical.”) (citation omitted). Courts and adjudicators must also consider whether

Significantly, transnational online conduct, harms, threats, and events will also be relevant to assessing the likelihood of future persecution. In the digital information environment, as well as with digital technologies such as surveillance, persecutors may reach across national boundaries to commit or incite harm. Post-flight online conduct, harms, threats, and events targeting an individual in a third country or the United States may be evidence of the persecutor's interest in harming an individual in the future, as well as his ability to do so.⁴⁸

For example, if Kate is threatened with physical harm on Twitter while in transit from her home country or after she arrives in New York, an agency or court must consider whether that threatening tweet is evidence that Kate is likely to be harmed if she were to return home.⁴⁹ As another example, assume that Kate's online presence is surveilled post-flight. An agency or court should similarly consider whether such post-flight, online surveillance is evidence that her government is likely to persecute her in the future.⁵⁰ It is crucial to remember that, in assessing

conduct and threats in the digital information environment are inherently persecutory because they are repetitive, viral, permanent, searchable, widely shared, and/or cumulative regardless of whether they involve or result in ancillary harms such as emotional trauma. See Jarvis Cooper, *Social Media & Online Persecution*, *supra* note 35, at 784–88.

48. Compare *Shulin Zhang v. Barr*, 831 F. App'x 41, 42–43 (2d Cir. 2020) (remanding to the agency to consider whether, due to surveillance, the asylum-seeker's government is likely to become aware of his post-flight online and offline activities); *Kyaw Zwar Tun v. INS*, 445 F.3d 554, 569–71 (2d Cir. 2006) (remanding to the agency to consider whether, due to post-flight, offline surveillance, the asylum-seeker's government is likely to become aware of his political activities), with *Guiyue Qian v. Lynch*, 629 F. App'x 81, 83 (2d Cir. 2015) (finding that, despite "record evidence" that the asylum-seeker's government monitors and blocks online activities, the government is not likely to discover the asylum-seeker's "limited" online activities); *Jiucheng Wen v. Holder*, 572 F. App'x 54, 56 (2d Cir. 2014) (holding that evidence of a government's digital surveillance within its borders does not mean that it surveils all dissident activities in the United States or online).

49. See, e.g., *Porras v. Holder*, 543 F. App'x 867, 874 & n.7 (10th Cir. 2013) (considering but rejecting the asylum-seeker's request to reconsider the denial of a motion to reopen asylum proceedings in which the asylum-seeker alleged a fear of future persecution due, in part, to post-flight, online threats).

50. See, e.g., *Yi Lun Wang v. Garland*, 857 F. App'x 679, 681–82 (2d Cir. 2021) (considering but rejecting such an assertion due to the insufficiency of the asylum-seeker's proffered evidence); *Guang Lin Chang v. U.S. Att'y Gen.*, 643 F. App'x 864, 868–69 (11th

whether persecution is likely to occur, an asylum-seeker only needs to present evidence that there is a ten percent chance of persecution in the future.⁵¹ In other words, Kate only needs to establish that the threatening tweet or online surveillance by themselves or in conjunction with other conduct, harms, threats, and events indicate a possibility—but not necessarily a certainty or probability—that she would be persecuted in the future.⁵²

Additionally, online conduct and harm in general may implicate the principle of non-refoulment under international law. This principle provides that countries cannot expel or return refugees to places where their life or freedom would be threatened on account of their race, religion, nationality, membership in a particular social group, or political opinion.⁵³ Thus, if conduct, harms, threats, and events attributable to the digital information environment indicate that an individual would be threatened on account of one or more of these identities in her home country, the United States may be prohibited under international law from forcing that individual to return home.⁵⁴ For example, returning to Kate, regardless of the time or place of the threatening tweet or online surveillance's initiation, such conduct may trigger a duty under international law to determine whether it is safe for Kate to return to her home country.⁵⁵

Cir. 2016) (similar); *Mei Qin Zheng v. Holder*, 538 F. App'x 51, 54 (2d Cir. 2013) (remanding to the agency to consider evidence supporting such an assertion).

51. See *INS v. Cardoza-Fonseca*, 480 U.S. 421, 440 (1987); see also *Al-Harbi v. INS*, 242 F.3d 882, 888 (9th Cir. 2001) (citing *INS v. Cardoza-Fonseca* and noting that "even a ten percent chance of persecution may establish a well-founded fear").

52. See *Hoxha v. Ashcroft*, 319 F.3d 1179, 1184 (9th Cir. 2003) ("A well-founded fear does not require certainty of persecution or even a probability of persecution.").

53. See *Convention Relating to the Status of Refugees*, art. 33, 28 Jul. 1951, 189 U.N.T.S. 137 (Apr. 22, 1954) [hereinafter the *Refugee Convention*].

54. In the United States, the relief of withholding of removal, as well as the legacy relief of withholding of deportation, are generally understood to reflect the principle of non-refoulment. See *INS v. Aguirre-Aguirre*, 526 U.S. 415, 419, 427 (1999) (citing *INS v. Cardoza-Fonseca*, 480 U.S. 421, 436–39 (1987) and *INS v. Stevic*, 467 U.S. 407, 414–16, 421–22 (1984)).

55. At a minimum, an individual like Kate in such a scenario may be eligible for the relief of withholding of removal. See *INS v. Aguirre-Aguirre*, 526 U.S. at 419, 427; see generally 8 U.S.C. § 1231; 8 C.F.R. §§ 208.16, 1208.16 (governing the relief of withholding of removal).

D. Emergence of Novel Harms

Asylum claims involving the digital information environment and accompanying technologies may produce novel harms because of the technology involved, as well as online users' behavior. Digital conduct and harm may even differ from its offline or analog counterpart. For example, online manipulation may be more subtle and effective than historical, offline forms of propaganda due to the ease of identifying and exploiting online users' vulnerabilities.⁵⁶ Consider digital surveillance as well: it differs from historical forms of surveillance, in part, because it involves automation and aggregation.⁵⁷ As scholar Andrew Guthrie Ferguson has explained, digital surveillance is always on and persistent.⁵⁸ The resulting injuries and repercussions from digital surveillance are also unique. For instance, while some individuals may self-censor due to digital surveillance,⁵⁹ others may be indirectly influenced to conform their online speech, conduct, and behavior to persecutors' mandates.⁶⁰

Novel digital conduct and harms may amount to more than harassment and even rise to the level of persecution under U.S. asylum law.⁶¹ To illustrate, let us return to Kate and assume that an online troll attacks her on Twitter for her political opinion. Due to the behavior of online users as well as Twitter's algorithms, that singular tweet may be shared thousands of times across the platform and even mutate into more vitriolic versions.⁶² The ease with which that one tweet can be amplified through widespread dissemination, proliferation of content, and mutation can compound Kate's emotional injury and elevate her fear of being harmed in the future. Due to the barrage of online attacks

56. See Daniel Susser et al., *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 17, 40–41 (2019).

57. See Andrew Guthrie Ferguson, *Persistent Surveillance*, 74 ALA. L. REV. 1, 16 (2022).

58. See *id.*

59. See, e.g., Clark & Grech, *supra* note 25, at 14.

60. See Penney, *supra* note 26, at 1454–55, 1458.

61. See *Gjetani v. Barr*, 968 F.3d 393, 397 (5th Cir. 2020) (noting that persecution differs from harassment).

62. See Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 134; Jarvis Cooper, *Social Media & Online Persecution*, *supra* note 35, at 774–75.

resulting in the compounding of Kate's emotional trauma and anxiety, Kate's experience of being attacked on Twitter is more than mere harassment.⁶³

Importantly, under U.S. asylum law, it is considered persecutory to be forced to conform or abandon one's opinions, beliefs, or identities as they relate to a protected characteristic, such as one's race, religion, nationality, membership in a particular social group, or political opinion.⁶⁴ Harms or threats in the digital information environment that chill an individual's expression of or identification with a protected characteristic may similarly be evidence of or even amount independently to persecution.⁶⁵ Put another way, online harms, threats, or manipulation that chill Kate's expression of or identification with a protected characteristic may be persecutory.⁶⁶

Given that the tools and methods of inflicting digital harm are constantly evolving in unpredictable and remarkable ways,⁶⁷ there are likely to be unprecedented and even unforeseeable legal and factual scenarios which may materialize in future asylum claims. The U.S. asylum system may thus be required to adapt existing asylum laws or devise different legal approaches to novel digital harms. Courts and adjudicators will also need to consider whether and when digital conduct and harm violates international law and when such violations are tantamount to persecutory harm under U.S. asylum law.⁶⁸ Additionally, the U.S.

63. See Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 125; Jarvis Cooper, *Social Media & Online Persecution*, *supra* note 35, at 795.

64. See *Aden v. Wilkinson*, 989 F.3d 1073, 1083 (9th Cir. 2021); *Kantoni v. Gonzales*, 461 F.3d 894, 898 (7th Cir. 2006); *Krotova v. Gonzales*, 416 F.3d 1080, 1086–87 (9th Cir. 2005); *Bucur v. INS*, 109 F.3d 399, 405 (7th Cir. 1997); see also *Mamouzian v. Ashcroft*, 390 F.3d 1129, 1137 n.6 (9th Cir. 2004).

65. See Liane M. Jarvis Cooper, *Privacy Harms and Persecution*, 31 S. CAL. INTERDISC. L.J. 469, 500–01 (2022) [hereinafter Jarvis Cooper, *Privacy Harms & Persecution*].

66. See *id.* at 473 (defining “online persecution” as “online conduct, manipulation, threats, words, or acts that are on account of a ground protected under U.S. asylum law and have resulted or may result in a sufficiently severe injury”).

67. See, e.g., Nair et al., *supra* note 33, at 238.

68. Cf. Deborah Anker & Sabi Ardalan, *Escalating Persecution of Gays and Refugee Protection: Comment on Queer Cases Make Bad Law*, 44 N.Y.U. J. INT'L L. & POL. 529, 539–42 (2012) (arguing that infringements, restrictions, or limitations on activities that

asylum law system will need to consider whether there may be circumstances in which digital conduct and harms warrant relief, remedy, or protection in the absence of offline harms, events, and circumstances.⁶⁹ For example, in addition to serving as evidence of future persecution,⁷⁰ tweets threatening death against Kate or violence against her fellow dissidents may be enough to constitute past persecution.⁷¹ In short, the digital information environment has unique characteristics that may produce novel ways of persecuting individuals and result in novel harms.

E. Unique and Disproportionate Targeting

Online, persecutors may target some individuals and groups more often and in a different manner than others.⁷² For instance, women may be targeted more often than men.⁷³ Take Kate. Following her tweet requesting political asylum, she may be more likely to be bombarded with multiple threats on social media than a male dissident because she identifies as a woman or, at least, her online attackers perceive her as a woman.⁷⁴ Women may also

are central to the enjoyment of a core or fundamental human right protected under international law may rise to the level of persecutory harm).

69. See Jarvis Cooper, *Social Media & Online Persecution*, *supra* note 35, at 781–82; Jarvis Cooper, *Privacy Harms & Persecution*, *supra* note 65, at 492–93.

70. See, e.g., *Flores Molina*, 37 F.4th at 630–40 (finding past persecution and remanding to the agency to reconsider its future persecution analysis where an asylum-seeker was threatened online and offline with violence and death); see also *Espinoza v. U.S. Att’y Gen.*, no. 23–1453, at 6 n.6 (3rd Cir., Dec. 1, 2023) (non-precedential) (noting that the agency observed that social media threats may be relevant to establishing a well-founded fear of future persecution but denying on other grounds).

71. See, e.g., *Flores Molina*, 37 F.4th at 630–40 (providing three bases to find past persecution where an asylum-seeker was threatened online and offline with violence and death); *Bedoya v. Barr*, 981 F.3d 240, 246–47 (4th Cir. 2020) (finding that multiple threats, including some via text message, amount to past persecution); see also Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 119.

72. See, e.g., Human Rights Watch, *supra* note 8, at 92, 520, 592, 604.

73. See JULIE POSETTI ET AL., *THE CHILLING: GLOBAL TRENDS IN ONLINE VIOLENCE AGAINST WOMEN JOURNALISTS* 16, 23–24 (UNESCO, 2021); Dubravka Šimonovic (Special Rapporteur on Violence Against Women, Its Causes and Consequences), *Online Violence Against Women and Girls from a Human Rights Perspective*, ¶28, U.N. Doc. A/HRC/38/47 (Jun. 18, 2018).

74. See, e.g., J. Nathan Matias et al., *Reporting, Reviewing, and Responding to Harassment on Twitter* 10 (Women, Action, & the Media, 2015), <https://doi.org/10.48550/arXiv.1505.03359>.

be subject to different content than men, as well as content that targets their multiple identities, such as their gender combined with their political opinion.⁷⁵ For example, online persecutors may attack Kate on multiple fronts, degrading not only her political opinion but also her gender and religious beliefs.

Individuals and groups may value and interact with the digital information environment and accompanying technologies differently than others. Targeted individuals' cultures, languages, ages, and other characteristics may influence how and why they interface with the digital information environment, including how they conceptualize, value, store, present, and access their digital identities and information, as well as how they perceive affronts to their digital identities and violations of their information norms.⁷⁶ For example, Kate may experience a doxing as more harmful than an individual with a different approach to data. As another example, age may affect how she perceives an attack on social media or a denigration of her online identity.

Individuals and groups may also be affected by digital harm differently depending upon their lived experiences. For instance, in comparison to individuals who are only targeted along one axis of identity, the resulting injuries may be compounded or more acute for individuals who are targeted on account of one or more identities such as gender interlocked with race. In other words, online harm may be unique and severe because it involves or is

75. See *Rodriguez Tornes v. Garland*, 993 F.3d 743, 755–57 (9th Cir. 2021) (Paez, J., concurring); see, e.g., Kiruba Munusamy, *Intersection of Identities: Online Gender and Caste-Based Violence*, GENDERIT.ORG (Jun. 7, 2018), <https://genderit.org/articles/intersection-identities-online-gender-and-caste-based-violence> [<https://perma.cc/R7XS-3ZU7>]; Emma Alice Jane, 'Back to the Kitchen, Cunt': *Speaking the Unspeakable About Online Misogyny*, 28 CONTINUUM: J. MEDIA & CULTURAL STUDS. 558, 565 (2014); see generally Kimberlé Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989(1) UNIV. CHI. LEG. FOR. 139, 149 (1989) (proposing the intersectionality framework).

76. See, e.g., Rina Diane Caballar, *How Indigenous Groups are Leading the Way on Data Privacy*, SCIENTIFIC AM., (Jun. 7, 2023), <https://www.scientificamerican.com/article/how-indigenous-groups-are-leading-the-way-on-data-privacy/> [<https://perma.cc/XU6Z-WYR3>]; Yao Li, *Cross-Cultural Privacy Differences*, in MODERN SOCIO-TECHNICAL PERSPECTIVES ON PRIVACY 267, 274–79 (Bart P. Knijnenburg et al. eds., 2022).

based on a targeted individual's intersecting identities, even raising it legally to the level of persecutory harm.⁷⁷

In the case of Kate, she may experience being bombarded by tweets attacking her race and gender more acutely than an individual who is only attacked on account of one identity. Thus, it will be critical for courts and agencies to consider online presence, conduct, harms, threats, and events through diverse cultural, religious, social, and intersectional frameworks. A failure to do so may obscure individuals' unique experiences of harm in the digital information environment.⁷⁸ Relatedly, such individuals must not be required to meet a higher standard of proof or persuasion relative to other targeted individuals.⁷⁹

F. Increased Significance of Non-State Actors

In the future, online users, moderators, and platforms are likely to figure more prominently in asylum claims.⁸⁰ One overarching issue that will arise in addressing asylum claims involving such actors and entities will be whether and under which circumstances they should be considered governmental persecutors.⁸¹ This is significant because a finding that such

77. Jarvis Cooper, *Sexual Privacy & Persecution*, *supra* note 26, at 132; *see also id.* at 130–32 (applying the intersectionality framework to online sexual privacy violations in the context of asylum claims). To read the intersectionality framework as originally proposed, *see* Crenshaw, *supra* note 75, at 149.

78. *See* Roxana Akbari & Stefan Vogler, *Intersectional Invisibility: Race, Gender, Sexuality, and the Erasure of Sexual Minority Women in US Asylum Law*, 46 L. & SOC. INQUIRY 1062, 1080–88 (2021) (documenting how the failure to embrace an intersectional framework may obscure sexual minority women's experiences of violence and persecution); *see also* Samuel Woolley, *Tech's Risks on Non-English Platforms*, DEMOCRACY (Spring 2023), <https://democracyjournal.org/magazine/68/techs-risks-on-non-english-platforms/> [<https://perma.cc/KC6L-3W78>] (emphasizing that online harm occurs in obscured digital spaces, such as WhatsApp, and in a multitude of languages other than English).

79. *Cf.* Anker & Ardalan, *supra* note 68, at 554–55 (raising similar concerns in the offline context and lamenting that the U.S. asylum law system's corroboration requirements and criteria for assessing credibility exceed the Refugee Convention's demands).

80. *See, e.g.*, Funk et al., *supra* note 25 (documenting the Chinese government's pressure on local and international platform companies to engage in restrictive, online measures).

81. *See* Jarvis Cooper, *Privacy Harms & Persecution*, *supra* note 65, at 481 n.104; *see generally* Molly K. Land, *Regulating Private Harms Online: Content Regulation under*

actors are governmental ones means that their conduct may be tantamount to governmental persecution. For instance, if the evidence shows that Kate's government engages online trolls to attack dissidents like Kate on social media,⁸² the trolls' online attacks may be considered governmental attacks. Let us examine another scenario. Assume, now, that rather than on Twitter, Kate posted on a platform run by or operating at the direction of her country's government.⁸³ If that platform surveilles her social media presence, that act may constitute governmental surveillance.

Another important issue will involve determining the degree to which a government is or was unable or unwilling to provide protection from harm committed or threatened by non-state online actors.⁸⁴ Let us assume that the online trolls who harmed or threatened Kate are non-state actors without a provable connection to her government. In such a scenario, Kate would need additionally to establish that her government is or was unable or unwilling to protect her from those online trolls.⁸⁵ In short, Kate would have an additional evidentiary burden to establish her claim of persecution.

In evaluating a government's ability and willingness to protect individuals from harm attributable to the digital information environment, there are several considerations to keep in mind. To begin with, such asylum claims, including the reasonableness of whether an individual could or should seek governmental protection, must be evaluated on a case-by-case basis.⁸⁶ There may be situations in which it is not reasonable to expect an individual to report the harm or threats emanating

Human Rights Law, in HUMAN RIGHTS IN THE AGE OF PLATFORMS 286–306 (Rikke Frank Jorgensen ed., 2019) (developing a typology to describe state activities in the digital information environment, as well as a framework under international human rights law for addressing the conduct of non-state, online content intermediaries).

82. See, e.g., OHCHR, *supra* note 13, at 14–15 (discussing governmental engagement of non-state actors to harm dissidents online).

83. See, e.g., Funk et al., *supra* note 25.

84. See generally Matter of C-G-T-, 28 I&N Dec. 740, 743 (BIA 2023) (explaining that “[w]hether a government is unable or unwilling to protect an individual from persecution is a question of fact”).

85. See *id.*

86. See *id.* at 744.

from the digital information environment.⁸⁷ For instance, a child may be less likely to seek assistance from the authorities.⁸⁸

Crucially, even if a targeted individual reports harmful online conduct to the authorities or there is some governmental responsiveness to online violence, neither scenario automatically equates to governmental ability and willingness to provide protection online and offline.⁸⁹ A country's customs or laws governing online conduct or harm may effectively deprive the individual or group of any meaningful recourse to governmental protection.⁹⁰ Imagine, for instance, in a country where violence against sexual minorities is culturally acceptable or certain gender identities are legally forbidden, that police may decline to investigate or prosecute online harms committed against individuals with such identities.⁹¹ Even where there are laws on the books, a government may be unwilling to provide protection due to its own animus or indifference towards the targeted individual or group.⁹² For example, even if there are laws against cyberstalking, police may decline to investigate online harms committed against individuals with certain religious backgrounds. Additionally, a government may lack the technological, policing, or other resources to provide protection even if it has the willingness to do so.⁹³

87. *Cf. id.* at 743.

88. *See id.*; *Portillo Flores v. Garland* 3 F.4th 615, 635–36 (4th Cir. 2021); *Bringas-Rodriguez v. Sessions*, 850 F.3d 1051, 1071 (9th Cir. 2017).

89. *J.R. v. Barr*, 975 F.3d 778, 782 (9th Cir. 2020) (making this argument in the context of offline harm).

90. *Doe v. U.S. Att'y Gen.*, 956 F.3d 135, 146–49 (3d Cir. 2020) (making this argument in the context of offline harm and citing *Bringas-Rodriguez v. Sessions*, 850 F.3d at 1066–67 and *Rahimzadeh v. Holder*, 613 F.3d 916, 922 (9th Cir. 2010)).

91. *See, e.g.*, Human Rights Watch, *supra* note 8, at 44, 70, 196, 205, 247, 263, 276, 300, 318–20, 349, 393, 420, 437, 456, 476, 492, 497–98, 592, 604, 613, 680, 706 (documenting such country conditions, including incidents in which the authorities in those countries failed to address online and offline harms).

92. *J.R.*, 975 F.3d at 782 (making this argument in the context of offline harm).

93. *Cf. id.* (noting in the offline context that “[w]illingness to control persecutors notwithstanding, authorities may nevertheless be ‘powerless to stop’ them because of a ‘lack of...resources’”) (citation omitted); *see, e.g.*, Human Rights Watch, *supra* note 8, at 168 (documenting an example of this phenomenon in the offline context).

G. Evidentiary Concerns

Courts and adjudicators must consider several issues when dealing with evidence in asylum claims involving the digital information environment. In engaging in the digital information environment, individuals may leave digital traces of themselves, including information about their online and offline connections; personal and group identities; beliefs and opinions; and geolocation and biometric identifiers.⁹⁴ These digital traces are seemingly permanent and may be readily discoverable and inferable, facilitating persecutors' ability to find and target individuals online and offline for their online content, communications, and activities.⁹⁵

However, despite digital evidence's portability and permanence, asylum-seekers may have limited abilities to retain and recall such evidence. As the Ninth Circuit has noted, "refugees sometimes are in no position to gather documentary evidence establishing specific or individual persecution or a threat of such persecution."⁹⁶ Consider Kate, for example. Her smartphone—and whatever she managed to document on it before fleeing her homeland—may be the extent of her evidence corroborating her past experience and future fears. It may also be too dangerous for individuals fleeing persecution to be caught with evidence on their smartphones or laptops.⁹⁷ Pre-flight, Kate may have even tried to eliminate digital evidence, fearing that the capture of such data could result in harm to her or loved ones back home.⁹⁸

Individuals in flight or post-flight may also not have access to tools to corroborate their experiences in the digital information

94. See Glowacka et al., *supra* note 2, at 4, 15; Marie Gillespie et al., *Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances*, 4(1) SOCIAL MEDIA + SOC'Y 1, 6, 9 (2018).

95. Cf. Gillespie et al., *supra* note 94, at 6, 9 (explaining that such digital traces may lead to offline harms).

96. *Cardoza-Fonseca v. INS*, 767 F.2d 1448, 1453 (1985), *aff'd* *INS v. Cardoza-Fonseca*, 480 U.S. 421 (1987); *see also* *Salaam v. INS*, 229 F.3d 1234, 1239 (9th Cir. 2000).

97. *See, e.g.*, Human Rights Watch, *supra* note 8, at 196, 349; Amnesty Int'l, *supra* note 8, at 194.

98. *See, e.g.*, Human Rights Watch, *supra* note 8, at 507.

environment.⁹⁹ “Authentic refugees rarely are able to offer direct corroboration of specific threats.”¹⁰⁰ Attempts to corroborate, authenticate, or retrieve digital evidence via contacts in an individual’s home country may be too dangerous, potentially endangering family and friends back home.¹⁰¹ It is thus important to refrain from under—or over—emphasizing the presence of digital evidence in asylum claims. In other words, in assessing a claim of persecution, courts and adjudicators must refrain from requiring or preferring digital evidence over other forms of credible evidence.¹⁰² And, finally, it is important to keep in mind

99. *Contra Mohamed v. Garland* 44 F.4th 761, 769, 771–72 (8th Cir. 2022) (faulting the withholding of removal applicant for failing to produce corroborating evidence of the online threats despite his testimony that he had encountered technical difficulties, and the digital information was either inaccessible or had been corrupted); *Pocasangre Garcia v. Garland*, no. 20-70307 at *3 (9th Cir., Jun. 7, 2021) (non-precedential, unpublished) (holding in a post-REAL ID Act case that the asylum-seeker did not adequately explain the unavailability of the threatening Facebook messages and never contacted Facebook for help in recovering the messages); see also *Uzodinma v. Barr*, 951 F.3d 960, 966–67 (8th Cir. 2020) (holding in a post-REAL ID Act case that, while the asylum-seeker explained that he could not access his social media accounts while incarcerated, additional notice and opportunity to obtain such corroborating evidence would not have changed the outcome of the proceedings); see generally REAL ID Act of 2005, Pub. L. 109–13, 119 Stat. 231 (2005) (amending the statutory provisions governing credibility determinations in asylum adjudications) [hereinafter the REAL ID Act].

100. *Bolanos-Hernandez v. INS*, 767 F.2d 1277, 1285 (9th Cir. 1984).

101. See, e.g., Human Rights Watch, *supra* note 8, at 507; see also Fiona B. Adamson & Gerasimos Tsourapas, *Coercion-by-Proxy as a Tool of Transnational Repression*, in PERSPECTIVES ON “EVERYDAY” TRANSNATIONAL REPRESSION IN AN AGE OF GLOBALIZATION 10 (Nate Schenkkan et al. eds., Freedom House 2020) (documenting how authoritarian regimes coerce dissidents living abroad by targeting their family members, associates, or acquaintances in the dissidents’ home countries); cf. Diane Uchimiya, *A Blackstone’s Ratio for Asylum: Fighting Fraud While Preserving Procedural Due Process for Asylum Seekers*, 26 PENN. ST. INT’L L. REV. 383, 391–92 (2007) (expressing similar concerns with authenticating asylum claims in the offline context).

102. See Koen Leurs & Kevin Smets, *Five Questions for Digital Migration Studies: Learning From Digital Connectivity and Forced Migration In(to) Europe*, 4(1) SOCIAL MEDIA + SOC’Y 8–10 (2018); see also Rikke Andreassen, *Social Media Surveillance, LGBTQ Refugees and Asylum: How Migration Authorities Use Social Media Profiles to Determine Refugees as ‘Genuine’ or ‘Fraudulent’*, 26(1) FIRST MONDAY (2021). Additionally, courts and adjudicators must consider that potential digital tools to assess the validity of asylum claims may be limited by the technology used, as well as the background of its developers and data-wranglers. See Matilda Arvidsson & Gregor Noll, *Decision Making in Asylum Law and Machine Learning*, 92(1) NORDIC J. INT’L L. 56, 84–89 (2023); see also Karen Weise & Cade Metz, *When A.I. Chatbots Hallucinate*, N.Y. TIMES (May 9, 2023), <https://www.nytimes.com/2023/05/01/business/ai-chatbots-hallucination.html>

that, like claims exclusively involving the offline realm, asylum-seekers' credible testimonies may alone, under certain circumstances, establish a claim of persecution.¹⁰³

H. Caseload and Fraud Concerns

Finally, the U.S. government must determine whether there is or will be an increase in genuine and fabricated claims involving the digital information environment and, if so, how it intends to address such an uptick.¹⁰⁴ At a minimum, the concern over an increase in asylum claims, as well as the capacity to handle such an increase, is not unique to claims involving the online realm.¹⁰⁵ The debate over the magnitude of fraud and its putative role in burdening the U.S. asylum system is similarly not limited to such claims.¹⁰⁶ Regardless of the extent of such concerns, the U.S. asylum system must preserve procedural due process by guarding against impermissibly raising the standard of proof or presuming fraud or incredibility in the adjudication of claims involving the digital information environment.¹⁰⁷ Lastly, it

[<https://perma.cc/UUN7-FWBX>] (raising concerns regarding the reliability of information produced by generative artificial intelligence systems and individuals' reliance on such systems for legal advice and decision-making).

103. See 8 U.S.C. § 1158(b)(1)(B)(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a); see also *Aden v. Holder*, 589 F.3d 1040, 1044 (9th Cir. 2009) (post-REAL ID Act); *Garrovillas v. INS*, 156 F.3d 1010, 1016–17 (9th Cir. 1998) (pre-REAL ID Act); *Matter of Mogharrabi*, 19 I&N Dec. 439, 445 (BIA 1987) (pre-REAL ID Act); cf. *Korniejew v. Ashcroft*, 371 F.3d 377, 382 (7th Cir. 2004) (pre-REAL ID Act).

104. See, e.g., *Y.C. v. Holder*, 741 F.3d 324, 338 (2d Cir. 2013) (raising such concerns).

105. See, e.g., *A Sober Assessment of the Growing U.S. Asylum Backlog*, Transactional Recs. Access Clearinghouse (Dec. 22, 2022), <https://trac.syr.edu/reports/705/> [<https://perma.cc/7HYT-EBVM>] (noting that the backlog of unadjudicated asylum claims is not new, although it continues to increase) [hereinafter TRAC Report]; see also *DHS v. Thuraissigiam*, 140 S. Ct. 1959, 2014 (2020) (Sotomayor, J., dissenting) (noting that “[i]t is universally acknowledged that the asylum regime is under strain”).

106. See, e.g., TRAC Report, *supra* note 105 (noting that the recent political, economic, and environmental instability in certain countries has contributed to an uptick in asylum claims); *Thuraissigiam*, 140 S. Ct. at 2014 & n.13 (Sotomayor, J., dissenting) (citing to agency testimony before Congress that various factors other than fraud may contribute to the pending case load before the immigration court system, including lengthy hiring times for new immigration judges and the continued use of paper files).

107. Cf. *Uchimiya*, *supra* note 101, at 384, 432 (raising these concerns in the offline context).

is important to keep in mind that all asylum-seekers must receive individualized analyses of their claims.¹⁰⁸

IV. CONCLUSION

As this essay has shown, online conduct, harms, threats, and events will present unique and novel issues which may challenge the development of judicial, regulatory, and policy frameworks to address asylum claims involving the digital information environment. These issues include the concomitant presence of online and offline harms, as well as past and future harms; the emergence of transnational persecution; the increased significance of non-state actors; the emergence of novel harms, as well as unique and disproportionate targeting of dissidents and marginalized individuals; and an increased focus on evidentiary, caseload, and fraud concerns.

To address these issues, the U.S. asylum system will benefit from soliciting the expertise of scholars and researchers in the fields of privacy law, digital repression studies, and digital migration studies, as well as other social science and technology-related disciplines.¹⁰⁹ Non-governmental organizations are also a critical resource for assessing presence, conduct, harms, threats, and events in the digital information environment.¹¹⁰ Federal agencies and Congress will similarly gain from seeking input from past and present asylum-seekers on their experiences in the asylum adjudication process and digital

108. See *Ordonez-Quino v. Holder*, 760 F.3d 80, 88 (1st Cir. 2014) (“[C]ourts usually assess whether harm rises to the level of persecution on a case-by-case basis.”); see also U.N. High Commissioner for Refugees, *Handbook on Procedures and Criteria for Determining Refugee Status and Guidelines on International Protection*, ¶¶ 51–53, U.N. Doc. HCR/1P/4/ENG/REV.4 (Feb. 2019).

109. For background on the fields of digital repression studies and digital migration studies, see generally Jennifer Earl et al., *The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review*, 8(10) SCIENCE ADVANCES 1, 2, 6 (2022); Kevin Smets et al., *Refugee and Mediated Lives*, in OXFORD RESEARCH ENCYCLOPEDIA OF COMMUNICATION (Oxford University Press, 2022).

110. For instance, such organizations may provide documented information about, as well as raise relevant questions for assessing, how and why persecutors, dissidents, and marginalized individuals in a particular country operate in the digital information environment. See, e.g., Shahbaz et al., *supra* note 8, at 37–43 (listing questions to assess the level of internet freedom in a country).

information environment. And, finally, federal agencies and Congress should strive to prevent the incorporation of biases, overgeneralizations, and other inaccuracies regarding asylum-seekers' experiences in the digital information environment into the administration of the U.S. asylum system and the development of statutes, regulations, and policies.¹¹¹

111. Cf. Anna R. Welch & Sara P. Cressey, *Due Process Denied: A Case Study from the Failures of the U.S. Affirmative Asylum*, HARV. INT'L L.J. PERSPECTIVES (Jun. 1, 2023), <https://journals.law.harvard.edu/ilj/2023/06/due-process-denied-a-case-study-on-the-failures-of-u-s-affirmative-asylum/> [<https://perma.cc/3VXM-HFRU>] (documenting biased decision-making, compassion fatigue, and burnout among Asylum Officers at the U.S. Department of Homeland Security's Boston Asylum Office).

