PRIVACY HARMS AND PERSECUTION

LIANE M. JARVIS COOPER*

ABSTRACT

Can a privacy violation be persecution? Despite a documented increase in global attacks on privacy, U.S. courts have not yet determined whether the victim of a privacy harm is eligible for asylum in the United States. This Article will propose several frameworks for addressing asylum claims alleging privacy harms. Under one novel framework, an online privacy harm may even amount to online persecution.

The Article has two thematic goals. The first goal is to begin the task of addressing privacy harms under U.S. asylum law. The second goal is to put the plight of asylum-seekers on the radar of privacy specialists by explaining why an asylum-seeker's privacy is valuable and worth protecting. These goals are critical because the plight of asylum-seekers is not esoteric or hypothetical: whether an individual receives asylum in the United States may be a matter of life or death.

I. INTRODUCTION

For an individual sitting in London or San Francisco, an attack on her privacy may result in reputational damage, personal angst, or financial ruin.[1] For another individual—especially if she is a member of a marginalized community—a privacy attack may result in additional threats, imprisonment, beatings, rape, or even death.[2] Can a privacy violation be persecution? Is the victim of a privacy harm eligible for asylum in the United States?

---

* 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 article are solely the author's and do not reflect those of any employers. The author would like to thank Gil Cooper, Ellen Liebowitz, and the editors of the *Southern California Interdisciplinary Law Journal*, including Juan Rehl-Garcia, Monica Mahal, and Eric Fram.

[1] *See, e.g.*, OFF. COMMC'NS, GOV'T OF THE U.K., INTERNET USERS' EXPERIENCE OF POTENTIAL ONLINE HARMS: SUMMARY OF SURVEY RESEARCH (2020), https://www.ofcom.org.uk/__data/assets/pdf_file/0024/196413/concerns-and-experiences-online-harms-2020-chart-pack.pdf (documenting online harms experienced by individuals in the United Kingdom); Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information (documenting online harms experienced by individuals in the United States of America).

[2] *See* HUM. RTS. WATCH, WORLD REPORT: EVENTS OF 2020 (2021), https://www.hrw.org/world-report/2021 [hereinafter HUM. RTS. WATCH, EVENTS OF 2020] (documenting the online harms and resulting offline injuries experienced by individuals from multiple countries); AMNESTY INT'L, *Toxic Twitter* (2018), https://www.amnestyusa.org/wp-content/uploads/2018/03/Toxic-Twitter.pdf (documenting online harms on social media and the resulting offline injuries experienced by individuals from multiple countries); *see also* Hum. Rts. Council, *Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Surveillance and Human Rights*, U.N. Doc. A/HRC/41/35, ¶1 (May 28, 2019) (expressing concerns that online surveillance has led to "arbitrary detention, sometimes to torture and possibly to extrajudicial killings").

Although privacy is considered a human right under international law,[3] U.S. courts have not yet addressed whether a privacy harm may amount to persecution under U.S. asylum law. Given that there is a documented increase in governmental and non-governmental attacks on privacy, especially in the online realm,[4] a framework must be developed under U.S. law to address asylum claims alleging privacy harms.

Drawing from the privacy harm typology developed by Danielle Keats Citron and Daniel J. Solove, this Article will provide an in-depth analysis of privacy harms in the context of asylum adjudications in the United States. The Article will propose three frameworks for addressing asylum claims involving privacy harms. Under the first framework, a privacy harm may serve as supporting evidence of past persecution. Under the second framework, a privacy harm may be evidence predicting future persecution. Under a third and novel framework, a privacy harm may qualify as persecution even if it is not accompanied by other harms, threats, acts, or events. Under the third approach, an online privacy harm may even amount to *online persecution*.[5]

This Article is divided into three parts. Part II will lay the groundwork for the proposed frameworks by defining offline and online persecution, providing an overview of courts' treatment of privacy-threatening conduct alleged in asylum claims, and introducing the privacy harm typology developed by Citron and Solove. Focusing on the online realm, Part III will then propose several frameworks for addressing privacy harms in asylum claims. Finally, Part IV will identify specific privacy harms that may be alleged in future asylum claims and discuss issues that may arise in addressing such harms.[6]

---

[3] *See* G.A. Res 217 (III) A, Universal Declaration of Human Rights, United Nations, art. 12 (Dec. 10, 1948) (declaring that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" and "[e]veryone has the right to the protection of the law against such interference or attacks"); *see also* G.A. Res 2200 (XXI) A, annex, International Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966); G.A. Res. 44/25, Convention on the Rights of the Child, art. 16 (Nov. 20, 1989); Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms,* art. 8 (Apr. 11, 1950) [hereinafter European Convention]; *see, e.g.*, Youth Initiative for Human Rights v. Serbia, App. No. 48135/06, ¶¶ 16, 22–26 (ECtHR June 25, 2013) (finding that online surveillance implicates Article 10 of the European Convention which includes the right "to receive and impart information and ideas without interference by public authority and regardless of frontiers").

[4] *See* ADRIAN SHAHBAZ & ALLIE FUNK, FREEDOM HOUSE, FREEDOM ON THE NET 2019: THE CRISIS OF SOCIAL MEDIA (2019), https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf [hereinafter SHAHBAZ & FUNK, *Social Media Surveillance*] (documenting the rise in governmental and non-state efforts at online surveillance on social media); *see also* ADRIAN SHAHBAZ & ALLIE FUNK, FREEDOM HOUSE, FREEDOM ON THE NET 2020: THE PANDEMIC'S DIGITAL SHADOW (2020), https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow (documenting that governments have used the Covid-19 pandemic as a pretext to ramp up online censorship and surveillance of their citizens).

[5] *See* Liane M. Jarvis Cooper, *Social Media and Online Persecution*, 35 GEO. IMMIGR. L.J. 749, 781–88 (2021) (proposing the concept of online persecution and explaining how conduct on social media may amount to online persecution); *see also* discussion *infra* Sections II.A, III.E.

[6] *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B. U. L. REV. 793, 831 (2022) [hereinafter Citron & Solove, *Privacy Harms*] (proposing a typology of privacy harms).

II. THE GROUNDWORK

Why is it important to consider privacy harms in the context of asylum adjudications? The answer is straightforward: a privacy harm may be evidence of past or future persecution. The privacy harm may even amount to persecution *by itself*. Significantly, an online privacy harm may be tantamount to *online persecution*. Thus, it is critical for both immigration and privacy specialists to have a good understanding of when and how privacy harms are implicated in asylum claims. For immigration specialists, understanding the nature of privacy harms and being able to identify such harms as persecutory will help in the adjudication of future asylum claims. In the context of asylum adjudications, many instances of "privacy harms" may also rise to the level of "persecutory harms."[7] Significantly, as internet use increases over time, future asylum claims are likely to involve allegations of online privacy harms, requiring U.S. federal courts and agency adjudicators to be adept at identifying those harms and the nature and severity of the injury to an asylum-seeker. For privacy specialists, understanding how privacy harms may arise in asylum claims will provide such scholars with real-world examples of the potentially devastating effects of offline and online privacy harms.[8]

Other scholars have noted that privacy-related harms may arise in asylum claims.[9] This Article continues the analysis by providing, for the first time, an in-depth analysis of privacy harms in the context of asylum adjudications in the United States, including the application of U.S. asylum precedents to such harms. Before devising a blueprint to address privacy harms in asylum claims, it is first necessary to delineate what is meant by "persecution" and "privacy harm." As such, the following sections will define persecution and privacy harm, as well as explore the courts' treatment of privacy-threatening conduct under U.S. asylum law thus far.

A. DEFINING OFFLINE AND ONLINE PERSECUTION

What is persecution? The Immigration and Nationality Act ("the INA" or "the Act") does not define "persecution."[10] However, the INA provides that an individual may be eligible for asylum if she establishes that she has a "well-founded fear of future persecution" on account of one of five protected grounds: race, religion, nationality, membership in a particular social group, or political opinion.[11] Despite the historical lack of a statutory definition, U.S. federal circuit courts and the Board of Immigration Appeals ("the

[7] *See* discussion *infra* Part IV.

[8] *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1091–92 (2002) (advocating a pragmatic, bottom-up approach to conceptualizing privacy that is based on particular contexts, rather than in the abstract); *see generally* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY, chap. 1 (Harvard University Press, 2008) (noting the need to explain the value of privacy and why it is worth protecting).

[9] *See, e.g.*, Scott Rempell, *Defining Persecution*, 2013 UTAH L. REV. 283, 294–95 (2013) (noting in general that "deprivations of liberty" and other "privacy harms," including those arising from surveillance, may amount to persecution under U.S. asylum law); *see also generally* James C. Hathaway & Michelle Foster, THE LAW OF REFUGEE STATUS 284–87 (2d ed. 2014) (discussing how privacy-related rights and harms may be implicated in refugee status determinations under international law).

[10] *See* 8 U.S.C. § 1101(a) (2022) (listing definitions for terms in the INA but not one for "persecution").

[11] *See* 8 U.S.C. §§ 1101(a)(42), 1158 (2022); 8 C.F.R. §§ 208.13, 1208.13 (2022).

Board" or "BIA")—the appellate body of the U.S. immigration court system—have, over the course of years, developed the concept of persecution. The First Circuit, for example, has noted that "[p]ersecution is a fluid term, not defined by statute" and "courts usually assess whether harm rises to the level of persecution on a case-by-case basis."[12] Along these lines, the Ninth Circuit has commented that persecution covers a range of harms and "[t]he determination that actions rise to the level of persecution is very fact-dependent."[13]

In January 2021, the U.S. Departments of Homeland Security and Justice ("DHS" and "the DOJ," respectively, and "the Departments," collectively) issued a final rulemaking with the intention of adding, for the first time, a definition of persecution to their respective regulations.[14] As of the publication of this Article, the rulemaking is enjoined from taking effect.[15] If the rulemaking were to take effect, the regulations would define persecution as "an intent to target a belief or characteristic, a severe level of harm, and the infliction of a severe level of harm by the government of a country or by persons or an organization that the government was unable or unwilling to control."[16] The intended regulatory language explains that persecution is "an extreme concept involving a severe level of harm that includes actions so severe that they constitute an exigent threat."[17] The regulatory language further lists several manifestations of harm or circumstances that will not amount to persecution.[18] Additionally, in the rulemaking's preamble, the Departments emphasize that a finding of persecution will be a rare occurrence.[19] The rulemaking does not discuss nor refer to "privacy harms."

Despite the Departments' recent regulatory efforts to define persecution narrowly, courts have historically and repeatedly expanded the potential universe of harms that may amount to persecution.[20] For example, courts have interpreted the INA as recognizing gender-based harms, including rape and female genital mutilation.[21] Congress has also acknowledged novel

[12] Ordonez-Quino v. Holder, 760 F. 3d 80, 87–88 (1st Cir. 2014) (citations omitted).

[13] Cordon-Garcia v. INS, 204 F.3d 985, 991 (9th Cir. 2000).

[14] *See* U.S. DEP'TS OF HOMELAND SEC. & JUSTICE, *Procedures for Asylum and Withholding of Removal; Credible Fear and Reasonable Fear Review*, 85 Fed. Reg. 80,274, 80,281, 80,385–86, 80,394–95 (Dec. 11, 2020) [hereinafter *Final Rule*] (proposing to add a definition of persecution at 8 C.F.R. §§ 208.1(e) and 1208.1(e)). The Departments both have jurisdiction over the relief of asylum. *See* 8 C.F.R. §§ 208.2, 1208.2 (2022). One route for applying for asylum involves filing affirmatively with DHS and being interviewed by an asylum officer with the U.S. Citizenship and Immigration Services ("USCIS"). *See id.* After being placed in deportation or removal proceedings before an Immigration Judge, an individual may also initiate or renew a previously filed asylum application. *See id.* An appeal of an Immigration Judge's decision may then be filed with the Board. *See* 8 C.F.R. § 1003.1 (2022). An asylum applicant may further appeal a Board decision with a U.S. federal circuit court. *See* 8 U.S.C. § 1252 (2022). Regardless of which Department has jurisdiction, the legal requirements for establishing asylum eligibility are generally the same. *See* U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13.

[15] *See* Pangea Legal Services (II) v. U.S. Dep't of Homeland Sec., 512 F. Supp. 3d 966, 969 (N.D. Cal. 2021).

[16] *Final* Rule, *supra* note 14, at 80,281, 80,386, 80,395.

[17] *Id.*

[18] *See id.*

[19] *See id.* at 80,327 (emphasizing that persecution is an "extreme concept").

[20] *See* Jarvis Cooper, *supra* note 5, at 778–79.

[21] *See, e.g.*, Avendano-Hernandez v. Lynch, 800 F.3d 1072, 1079 (9th Cir. 2015) (recognizing rape and sexual assault as persecutory harm); Abebe v. Gonzales, 432 F.3d 1037, 1042 (9th Cir. 2005) (en banc) (recognizing female genital mutilation as persecutory harm); Nakibuka v. Gonzales, 421 F. 3d 473, 477 (7th Cir. 2005) (recognizing the threat of rape as persecutory harm); Hernandez-Montiel v. INS, 225 F.3d 1084, 1097 (9th Cir. 2000) (recognizing rape as persecutory harm), *overruled on other grounds by* Thomas v. Gonzales, 409 F.3d 1177, 1187 (9th Cir. 2005).

harms as persecution. For instance, Congress amended the INA to recognize that experiencing or fearing a forced abortion or involuntary sterilization due to a country's coercive population control program is persecution.[22] Short of a radical break with the courts' historical approach of recognizing novel harms as persecutory, there is no basis in law or logical reason for courts or agency adjudicators to exclude privacy harms categorically from the concept of persecution. Additionally, given that the Departments note in the rulemaking's preamble that asylum claims will continue to be analyzed on a case-by-case basis,[23] there is room under the potential, regulatory definition of persecution for the possibility that, depending upon the circumstances in an asylum claim, a privacy harm may amount to persecution.[24] Thus, showing flexibility and openness to viewing privacy and data-related harms as persecutory would align with U.S. asylum law's historical approach to recognizing novel harms as persecutory.

What is online persecution? Given that future asylum claims are likely to involve online conduct and harms, it is necessary to describe or categorize such phenomena under U.S. asylum law. As there is no statutory, regulatory, or judicial guidance on such phenomena, I propose a working definition of online persecution to describe the interplay between online conduct and harm. To be useful for practitioners of U.S. asylum law, the definition is derived from terms used in the INA and its implementing regulations, as well as established asylum precedents.[25] Thus, I define "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.[26] By "online," I intend to include the full range of digital technologies, including those that exist on the internet, in the cloud, and via other networked and smart devices, digital assistants, and communication channels.[27] By "conduct," I intend to include, at a minimum, what Jacqueline D. Lipton refers to as privacy-threatening invasions and

[22] *See* Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104–208, 110 Stat. 3009-546, § 601 (Sep. 30, 1996) (amending 8 U.S.C. § 1101(a)(42) to recognize such harms as persecution on account of a political opinion); *see also* Matter of S-L-L-, 24 I&N Dec. 1, 5–7 (BIA 2006) (applying the Congressional amendments).

[23] *See Final Rule*, *supra* note 14, at 80,328.

[24] In other areas of law where privacy harms are considered novel, such as the national security context, courts are similarly considering whether privacy and data-related harms may necessitate relief or remedy. *See, e.g.*, Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 431, 438 (2017) (explaining that, in the national security context, U.S. courts appear to be prepared to recognize as harmful the interception of content, database storage and analysis, and a wider array of data-related harms).

[25] In addition to this Article's definition of online persecution, bad actors' online conduct has been described variously as "digital repression," "digital persecution," and "digital authoritarianism." *See, e.g.*, STEVEN FELDSTEIN, THE RISE OF DIGITAL REPRESSION: HOW TECHNOLOGY IS RESHAPING POWER, POLITICS AND RESISTANCE 25 (2021); Louis Edward Papa & Thaier Hayajneh, *A Survey of Defensive Measures for Digital Persecution in the Global South*, 12 FUTURE INTERNET 166 (2020), https://doi.org/10.3390/fi12100166; ADRIAN SHAHBAZ, FREEDOM HOUSE, FREEDOM ON THE NET 2018: THE RISE OF DIGITAL AUTHORITARIANISM (2018), https://freedomhouse.org/sites/default/files/2020-02/10192018_FOTN_2018_Final_Booklet.pdf. While these descriptions are highly useful in other contexts, I have chosen to use "persecution" because it is a distinct, albeit evolving, concept under U.S. asylum law.

[26] *See* Jarvis Cooper, *supra* note 5, at 781–88 (proposing the concept of online persecution and explaining how conduct on social media may amount to online persecution).

[27] *See, e.g.*, Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1240, 1270–78 (2017) (explaining how digital assistants can be used as tools to control or block access to content, manipulate people's ideas, and amplify some ideas over others).

uses.[28] Uses include those identified by Solove, such as information collection, information processing, and information dissemination.[29] Conduct may, of course, also include online behavior and acts that do not necessarily implicate an individual's privacy. For example, online conduct also includes "dogpiling"—the phenomenon on social media in which many users concurrently attack a victim, often as a part of a campaign or coordinated attack.[30]

Now that significant terms have been defined, let us return to the question at hand: Can a privacy harm be indicative of persecution? As will be discussed in the next section, U.S. courts have not yet specifically addressed whether a privacy harm may amount to persecution.

B. COURTS' TREATMENT OF PRIVACY-THREATENING CONDUCT IN ASYLUM CLAIMS

U.S. asylum law has yet to recognize privacy harms as persecution. However, courts have occasionally recognized that part of the trauma that an individual experienced in the past or fears in the future may be due to an incursion into her privacy. Most of these cases have dealt with conduct perpetrated or threatened against an individual's body and physical integrity. By contrast, courts have rarely invoked the concept of privacy in addressing asylum claims involving surveillance, censorship, or nonbodily intrusions.

Courts have overwhelmingly found that conduct such as sexual assault, rape, and female genital mutilation may amount to persecution.[31] Courts have additionally found that forced gynecological examinations and procedures may constitute persecution.[32] Occasionally, as part of the analyses, courts have recognized—or, at least, implied—that conduct that violates an individual's body may *also* implicate her privacy.[33] For example, in explaining why rape is persecutory, the Ninth Circuit emphasized that one of the "hallmarks" of persecutory conduct is "the violation of bodily integrity and bodily autonomy."[34] As another example, in addressing the childhood experience of having one's genitals forcibly exposed, the Seventh Circuit noted that it "cannot conceive of a more basic subject of privacy than the naked body."[35] The court went on to explain that "the desire to shield one's unclothed figure from [the] view of strangers . . . is impelled by

[28] *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 499 (2010).

[29] *See* Daniel J. Solove, *A Taxonomy of Privacy*, U. PENN L. REV. 477, 488 (2006).

[30] *See* J. NATHAN MATIAS, AMY JOHNSON, WHITNEY ERIN BOESEL, BRIAN KEEGAN, JACLYN FRIEDMAN & CHARLIE DETAR, WOMEN, ACTION, & THE MEDIA, REPORTING, REVIEWING, & RESPONDING TO HARASSMENT ON TWITTER 10 (May 13, 2015), https://arxiv.org/ftp/arxiv/papers/1505/1505.03359.pdf (describing dogpiling on Twitter).

[31] *See, e.g.*, Avendano-Hernandez v. Lynch, 800 F.3d 1072, 1079 (9th Cir. 2015) (rape and sexual assault); Abebe v. Gonzales, 432 F.3d 1037, 1042 (9th Cir. 2005) (en banc) (female genital mutilation).

[32] *See, e.g.*, Mei Fun Wong v. Holder, 633 F.3d 64, 72 (2d Cir. 2011); Li v. Ashcroft, 356 F.3d 1153, 1158 (9th Cir. 2004) (en banc).

[33] *See, e.g.*, *Mei Fun Wong*, 633 F.3d at 72; Kholyavskiy v. Mukasey, 540 F.3d 555, 570 (7th Cir. 2008); Li v. Gonzales, 405 F.3d 171, 179 (4th Cir. 2005). *Cf.* Fatma E. Marouf, *The Rising Bar for Persecution in Asylum Cases Involving Sexual and Reproductive Harm*, 22 COLUM. J. GENDER & L. 81, 85–86 (2011) [hereinafter Marouf, *Sexual and Reproductive Harm*] (arguing that courts have overlooked privacy harms in cases involving female genital mutilation and the involuntary insertion of an intrauterine contraceptive device).

[34] Kaur v. Wilkinson, 986 F.3d 1216, 1222 (9th Cir. 2021).

[35] *Kholyavskiy*, 540 F.3d at 570 (citations omitted).

elementary self-respect and personal dignity."[36] Similarly, in a coercive population control case, the Second Circuit explained that the involuntary insertion of an intrauterine contraceptive device "involves a serious violation of personal privacy and deprives a woman of autonomy in making decisions about whether to bear a child."[37] Recognizing that a privacy harm can be ongoing, Judge Roger L. Gregory explained in a dissenting opinion in *Li v. Gonzales* that the Chinese government's forced insertion and continued required usage of an intrauterine contraceptive device constituted "both a violation of [asylum-seeker] Li's personal bodily privacy *and* a continuing invasion of that privacy."[38]

By contrast, courts evaluating asylum claims involving offline surveillance have rarely focused on the issue of privacy.[39] Rather, courts have usually scrutinized two issues: (1) whether past incidents of offline surveillance may contribute to a finding of cumulative or overall past persecution;[40] and (2) whether such conduct is a harbinger of future persecution.[41] Courts have been divided over whether surveillance may be evidence of persecution.[42] On the one hand, courts have recognized that surveillance can contribute to a finding of cumulative or overall past persecution and may even amount to persecutory harm by itself.[43] Courts have also found that past surveillance may lead to future persecution.[44] Courts have even opined that surveillance of asylum-seekers or other individuals *after* the asylum-seekers have left their home country may indicate a likelihood of future persecution.[45] Significantly, the Ninth Circuit

[36] *Id.* (citations omitted) (ellipsis in the original).

[37] *Mei Fun Wong*, 633 F.3d at 72.

[38] *Li v. Gonzales*, 405 F.3d at 183 (Gregory, J., dissenting) (emphasis in the original). Additionally, in finding that a forced gynecological exam was persecutory, the Ninth Circuit hinted that such conduct may implicate the asylum-seeker's sexual privacy. *See, e.g.*, Li v. Ashcroft, 356 F.3d 1153, 1158 & 1158 n. 4 (9th Cir. 2004) (en banc) (finding that the asylum-seeker's forced pregnancy exam at the hands of the government, which the asylum-seeker described as "rape-like," amounted to persecution because it involved both a physical invasion and emotional trauma). *But see* Ru Lin v. U.S. Att'y Gen., 223 F. App'x 91, 92–94 (3d Cir. 2007) (distinguishing *Li v. Ashcroft* and declining to find persecution where government officials repeatedly demanded that the asylum-seeker undergo such an examination which she refused because she believed it violated her right of privacy as well as basic human rights).

[39] *Cf.* Gomez-Zuluaga v. U.S. Att'y Gen., 527 F.3d 330, 342 (3d Cir. 2008) (noting, but not emphasizing in the persecution determination, that in-person surveillance was "certainly threatening and violative of the Petitioner's privacy").

[40] *See, e.g.*, Kazemzadeh v. U.S. Att'y Gen., 577 F.3d 1341, 1353 (11th Cir. 2009) (finding that in-person surveillance, along with other offline harms, does not compel a finding of past persecution); *Gomez-Zuluaga*, 527 F.3d at 342 (finding that, while in-person surveillance, under the circumstances, did not rise to the level of past persecution, an eight-day abduction did); Zheng v. U.S. Att'y Gen., 451 F.3d 1287, 1291 (11th Cir. 2006) (finding that, under the circumstances, in-person surveillance did not compel a finding of past persecution).

[41] *See, e.g.*, Chavarria v. Gonzalez, 446 F.3d 508, 521–22 (3d Cir. 2006) (finding that an asylum-seeker's fear of future persecution is objectively reasonable because he was surveilled and attacked in the context of documented human rights abuses against political dissidents).

[42] *Compare Kazemzadeh*, 577 F.3d at 1353, *Zheng,* 451 F.3d at 1291, *with Gomez-Zuluaga*, 527 F.3d at 342, *Chavarria*, 446 F.3d at 521–22.

[43] *See, e.g.*, Manzur v. U.S. Dep't of Homeland Sec., 494 F.3d 281, 292–93 (2d Cir. 2007) (finding that surveillance amounted to past persecution); *see also* Begzatowski v. INS, 278 F.3d 665, 669 (7th Cir. 2002) (noting in dicta that surveillance is a type of harm that might "cross the line" from harassment to persecution) (citing Mitev v. INS, F.3d 1325, 1330 (7th Cir. 1995)).

[44] *See, e.g.*, Ayele v. Holder, 564 F.3d 862, 871 (7th Cir. 2009); Zhao v. Mukasey, 540 F.3d 1027, 1030–31 (9th Cir. 2008); Tagaga v. INS, 228 F.3d 1030, 1034 (9th Cir. 2000); Nasseri v. Moschorak, 34 F.3d 723, 727–28, 729–30 (9th Cir. 1994).

[45] *See* Kyaw Zwar Tun v. INS, 445 F.3d 554, 569–71 (2d Cir. 2006) (citing evidence that the Burmese government surveils dissidents in the United States and finding that post-flight surveillance

has noted that persecutors may surveil individuals *because* of their political opinion or other protected identity.[46]

On the other hand, courts have sometimes found that surveillance does *not* contribute to a finding of past persecution.[47] In these cases, courts have held that surveillance either alone or in conjunction with other circumstances does not rise to the level of past persecution.[48] Courts have sometimes minimized the past surveillance by characterizing it as "periodic questioning"[49] or "mere harassment."[50] Other times, courts have opined that surveillance does not necessarily indicate a likelihood of future persecution.[51] Additionally, courts have denied asylum claims involving offline surveillance for other reasons, such as finding that the claims lack credibility,[52] plausibility,[53] or corroboration.[54]

Outside the context of asylum, online surveillance is often viewed as raising privacy concerns.[55] However, in the asylum context, courts have not specifically addressed whether online surveillance, censorship, or any other online conduct implicates privacy concerns. Instead, in cases addressing online surveillance, the inquiry has usually focused on whether, due to such monitoring, the persecutor is likely to discover the asylum-seeker's online presence and consequently be interested in harming her because of her online or offline conduct, beliefs, opinions, or identity.[56] Even in the face of admittedly "record" evidence of online surveillance, courts have found that the persecutor is *not* likely to discover the asylum-seeker's online presence or be interested in harming her.[57] In denying motions to reopen proceedings, courts have similarly found that, despite the existence of persecutors' post-proceedings online surveillance in the home country, conditions in the country had not changed increasing the likelihood of future persecution.[58] In one non-precedential decision, the Eleventh Circuit also denied a motion alleging that there had been an increase in online surveillance targeted at individuals outside the physical borders of the asylum-seeker's home

of an asylum-seeker is evidence of future persecution); Zhang v. Ashcroft, 388 F.3d 713, 718 (9th Cir. 2004) (finding, in a withholding of removal case, that post-flight surveillance of an asylum-seeker's family remaining in their home country is indicative of future harm).

[46] *See, e.g.*, *Nasseri*, 34 F.3d at 730.

[47] *See, e.g.*, Kazemzadeh v. U.S. Att'y Gen., 577 F.3d 1341, 1353 (11th Cir. 2009); Zheng v. U.S. Att'y Gen., 451 F.3d 1287, 1291 (11th Cir. 2006); Roman v. INS, 233 F.3d 1027, 1034 (7th Cir. 2000).

[48] *See, e.g.*, *Kazemzadeh*, 577 F.3d at 1353; *Zheng,* 451 F.3d at 1291; *Roman*, 233 F.3d at 1034; *see also* Gomez-Zuluaga v. U.S. Att'y Gen., 527 F.3d 330, 342 (3d Cir. 2008) (noting that, under the circumstances, surveillance alone does not rise to the level of past persecution) (citing Chavarria v. Gonzalez, 446 F.3d 508, 519 (3d Cir. 2006)).

[49] *See, e.g.*, Tao Chen v. Lynch, 810 F.3d 466, 475–76 (7th Cir. 2016).

[50] *See, e.g.*, *Kazemzadeh*, 577 F.3d at 1353; *Zheng,* 451 F.3d at 1291. *But see* Begzatowski v. INS, 278 F.3d 665, 669 (7th Cir. 2002).

[51] *See, e.g.*, *Tao Chen*, 810 F.3d at 475–76; Tamas-Mercea v. Reno, 222 F.3d 417, 426–27 (7th Cir. 2000).

[52] *See, e.g.*, Pop v. INS, 270 F.3d 527, 531–32 (7th Cir. 2001); *see also* Yue Cai v. Holder, 603 F. App'x 51, 53–54 (2d Cir. 2015).

[53] *See, e.g.*, He Chen v. Holder, 457 F. App'x 1, 3 (1st Cir. 2012).

[54] *See, e.g.*, *Tao Chen*, 810 F.3d at 475–76.

[55] *See generally* Citron & Solove, *Privacy Harms*, *supra* note 6.

[56] *See, e.g.*, Y.C. v. Holder, 741 F.3d 324, 328, 333–34, 336–37 (2d Cir. 2013); *see also* Yi Lun Wang v. Garland, No. 19-2643 NAC *3–4, 7–8 (2d Cir. May 6, 2021); Guiyue Qian v. Lynch, 629 F. App'x 81, 83 (2d Cir. 2015); Jiucheng Wen v. Holder, 572 F. App'x 54, 56 (2d Cir. 2014); Mei Qin Zheng v. Holder, 538 F. App'x 51, 54 (2d Cir. 2013).

[57] *See, e.g.*, *Guiyue Qian*, 629 F. App'x at 83; *Jiucheng Wen*, 572 F. App'x at 56.

[58] *See, e.g.*, Feng Zheng v. U.S Att'y Gen., 569 F. App'x 757, 758–59 (11th Cir. 2014); Bin Chen v. U.S. Att'y Gen., 360 F. App'x 95, 97 (11th Cir. 2010).

country.[59] Additionally, courts have denied claims involving online surveillance because the claims were not sufficiently corroborated[60] or lacked credibility[61] or plausibility.[62] In contrast to courts' characterization of offline surveillance as "mere harassment" that does not rise to the level of persecution,[63] courts have not discussed whether online surveillance could or should be labelled as harassment. Significantly, courts have not addressed the *nature* or *severity* of privacy harms resulting from online surveillance.

In the few cases that have directly addressed offline censorship, courts have not discussed privacy concerns. Rather, courts have focused on other issues or characterizations of the offline censorship. For example, in one non-precedential case, the Ninth Circuit found that, depsite circulating books about a persecuted religious group, an asylum-seeker only faced potential "punishment" under China's censorship laws, not persecution.[64] In a different, non-precedential case, however, the Ninth Circuit regarded journalists' self-censorship as evidence of a persecutory environment in the asylum-seeker's home country.[65]

Online censorship cases have also not addressed privacy-related concerns. In those cases, which have often involved motions to reopen proceedings, courts have focused on whether, due to the persecutor's post-proceedings online censorship and surveillance, as well as his offline conduct, conditions have changed in the asylum-seeker's country increasing the likelihood of future persecution.[66] In denying the motions, courts have sometimes minimized the significance of the online censorship and surveillance, characterizing such conduct as a *continuation* or *extension* of the offline persecution that does not necessitate reopening proceedings.[67] As the Second Circuit noted in the non-precedential decision *Qing Chen v. U.S. Att'y Gen*, "the Chinese Government's efforts to control activism via the internet is merely part of its ongoing history of suppressing dissent and controlling the dissemination of barred ideas and material."[68] Like the cases dealing with online surveillance, courts have also not addressed the nature or severity of the privacy harm resulting from online censorship.

Thus, courts have provided little guidance on what is meant by a "privacy harm" in the context of asylum. Before addressing how privacy

---

[59] *See, e.g.*, Guang Lin Chang v. U.S. Att'y Gen., 643 F. App'x 864, 868–69 (11th Cir. 2016).

[60] *See, e.g.*, Zhi Hui Zhu v. Barr, 767 F. App'x 58, 60 (2d Cir. 2019); *Guang Lin Chang*, 643 F. App'x at 868–69; *Guiyue Qian*, 629 F. App'x at 83.

[61] *See, e.g.*, Siang Piow Liu v. Holder, 403 F. App'x 207, 207–08 (9th Cir. 2010); Hui Zhu v. Holder, 331 F. App'x 36, 38 (2d Cir. 2009).

[62] *See, e.g.*, Yong Hua Jiang v. Lynch, 640 F. App'x 33, 35 (2d Cir. 2016); *Guiyue Qian*, 629 F. App'x at 83.

[63] Kazemzadeh v. U.S. Att'y Gen., 577 F.3d 1341, 1353 (11th Cir. 2009) (citation omitted); *see also* Zheng v. U.S. Att'y Gen., 451 F.3d 1287, 1291 (11th Cir. 2006) (similar).

[64] *See* Suping Ding v. Gonzales, 234 F. App'x 418, 419–20 (9th Cir. 2006).

[65] *See* Avetisyan v. Gonzales, 177 F. App'x 760, 762 (9th Cir. 2006) (finding past persecution in a case in which a journalist was beaten and raped and noting that the evidence indicated that journalists who do not self-censor suffer retaliation).

[66] *See, e.g.*, Ming Chen v. Holder, 722 F.3d 63, 67–68 (1st Cir. 2013); *see also* Feng Zheng v. U.S Att'y Gen., 569 F. App'x 757, 758–59 (11th Cir. 2014); Qing Chen v. U.S. Att'y Gen., 428 F. App'x 212, 214–15 (3d Cir. 2011); Xian Jiang Dong v. Holder, 379 F. App'x 54, 55–56 (2d. Cir. 2010).

[67] *See, e.g.*, *Ming Chen*, 722 F.3d at 68 (characterizing the Chinese government's "purported desire to control" the internet as "entirely consistent with its general approach toward pro-democracy activism"); *see also Qing Chen*, 428 F. App'x at 214–15; *Xian Jiang Dong*, 379 F. App'x at 55–56.

[68] *Qing Chen*, 428 F. App'x at 215.

harms may arise in future asylum claims, especially those involving the online realm, it is first necessary to identify and define different types of privacy harms.

C. DEFINING PRIVACY HARMS

What are "privacy harms"? Outside the context of U.S. asylum law, Citron and Solove have developed a typology of privacy harms, arguing that many of these harms should be recognized as warranting relief or a remedy.[69] While there are other conceptualizations of privacy,[70] Citron and Solove's typology provides a useful and pragmatic framework for discussing how privacy harms—especially those related to the online realm—are likely to arise in asylum claims. The following privacy harms are illustrative of those that may be alleged in future asylum claims: economic harms; psychological harms; lack of control harms; chilling effect harms; and manipulation harms.[71] To understand how these privacy harms may arise in asylum claims, it is critical to define such harms.

Let us start with economic privacy harms. Privacy violations can cause financial or monetary losses.[72] For example, identity theft victims whose stolen personal data has been used to conduct fraudulent transactions may suffer direct financial losses.[73] In addition, while not yet recognized by the courts as cognizable harms, privacy violations may also involve the loss of opportunities rather than direct financial injuries.[74] For example, a victim of identity theft may lose productivity and time clearing up the fraudulent debt.[75]

Privacy violations may also cause emotional and psychological trauma.[76] As Citron and Solove explain, such harms may involve anxiety, anguish, concern, irritation, disruption, or aggravation.[77] Citron and Solove categorize these wide array of feelings into two general categories—"emotional distress" which involves "painful or unpleasant feelings" and "disturbance" which involves "disruption to tranquility and peace of mind."[78] Notably, courts have recognized that emotional distress may be the *sole* basis of harm under four privacy torts: intrusion upon the plaintiff's seclusion; public disclosure of embarrassing private facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; and appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[79]

---

[69] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 799, 830–31.

[70] *See* Jeffrey M. Skopek, *Untangling Privacy: Losses Versus Violations*, 105 IOWA L. REV. 2169, 2175–81 (2020) (providing an overview of normative and descriptive accounts of privacy). *See, e.g.,* Ignacio N. N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1048 (2018) (providing a descriptive account in which privacy is conceived of as involving the limiting of access to personal information, control over information, and appropriate information flows).

[71] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 831, 834–37, 841–48, 853–55.

[72] *See id.* at 834.

[73] *See id.* at 834–35.

[74] *See id.* at 834.

[75] *See id.* at 834–35 (noting that, in other contexts, such as the loss of consortium, courts readily recognize the loss of productivity and time as cognizable harms).

[76] *See id.* at 841.

[77] *Id.*

[78] *Id.*

[79] *See id.* at 809, 842–43 (citation omitted).

In addition to economic and emotional injuries, privacy violations may result in autonomy harms.[80] Autonomy harms occur when individuals' choices are restricted, undermined, inhibited, or unduly influenced.[81] Such harms occur when "[p]eople are either directly denied the freedom to decide or are tricked into thinking that they are freely making choices when they are not."[82] Under Citron and Solove's typology, there are several subtypes of autonomy harms.[83]

One subtype of autonomy harm involves the lack or loss of control over one's personal data or information.[84] In Citron and Solove's conceptualization, the crux of this privacy harm is the undermining of an individual's ability to make meaningful choices about her data or prevent the potential future misuse of it, regardless of whether the individual's data is actually circulated or shared or the misuse of the data results in additional harms.[85] Citron and Solove explain that losing control over one's personal data impairs an individual's "peace of mind" and her "ability to manage risk."[86] This injury may arise, for example, when a company uses or retains an individual's data in violation of a statutory restriction or right.[87] While courts have been inconsistent in recognizing the loss of control as a harm, Citron and Solove argue that such an injury should be acknowledged as a cognizable harm.[88]

Another subtype of autonomy harm involves chilling effects in which the privacy violation deters or inhibits an individual from engaging in certain activities.[89] Citron and Solove list the exercise of free speech and association, political participation, religious practice, the expression of beliefs, and the exploration of ideas as examples of activities that could be potentially chilled or inhibited by another's privacy-threatening conduct.[90] In the United States, chilling effects are often discussed in the context of the First Amendment.[91] Significantly, as Jonathon W. Penney has explained, chilling effects may not only deter an individual from engaging in her preferred activities but may also influence her to conform her speech, conduct, or behavior to perceived social norms, thereby shaping her identity.[92]

---

[80] *See id.* at 845–61.
[81] *Id.* at 845.
[82] *Id.*
[83] *See id.* at 845–46.
[84] *See id.* at 853–54.
[85] *See id.* at 846, 853–54.
[86] *Id.* at 853.
[87] *See id.*
[88] *See id.* at 853–54.
[89] *See id.* at 846, 854–55 (defining chilling effects as "inhibiting people from engaging in lawful activities"). *See generally* Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 125–34 (2016) [hereinafter Penney, *Online Surveillance and Wikipedia Use*] (explaining that chilling effects theory is "the idea that government laws or actions might chill people's free activities" and providing an overview of chilling effects theory).
[90] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 854.
[91] *See id.*
[92] *See* Jonathon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. (forthcoming 2022), manuscript at 105–06, 109, 175–76, *available at* https://ssrn.com/abstract=3855619 (proposing a social conformity theory of chilling effects).

Finally, privacy violations may involve manipulation.[93] While manipulative conduct may affect consumers' decision-making,[94] it may also give rise to more fundamental and consequential harms by robbing individuals of their freedom to decide political, religious, social, and cultural matters.[95] For example, an individual may be manipulated in how she votes, altering the outcome of an election.[96]

While the harms discussed here do not necessarily represent the full range of privacy harms that may be implicated in asylum claims, the selected harms are a good place to start. The following Part will lay out three potential frameworks for addressing privacy harms in asylum adjudications.

III. CONCEPTUALIZING PRIVACY HARMS UNDER U.S. ASYLUM LAW

There are several ways to address asylum claims alleging that a persecutor's conduct has resulted or may result in privacy harms. Two conceptualizations can be easily mapped onto existing U.S. asylum law and themes. Under one conceptualization, a privacy harm serves as supporting evidence of past persecution. Under a second conceptualization, conduct that has or may offend, violate, or threaten an individual's privacy may be evidence of future persecution. Under a third and novel conceptualization, a privacy harm is sufficiently severe to amount to a persecutory harm, even if it is not connected to other harms, threats, acts, or events. Under this last approach, a privacy harm *by itself* may amount to persecution and, correspondingly, an online privacy harm may amount to *online persecution*. All three conceptualizations require evidence establishing the elements of an asylum claim.

A. MAPPING PRIVACY HARMS ONTO THE ELEMENTS OF AN ASYLUM CLAIM

Under U.S. asylum law, an individual may be eligible for asylum if she has been or may be persecuted on account of one of five protected grounds—race, religion, nationality, membership in a particular social group, or political opinion.[97] The U.S. Supreme Court has held that an individual's fear of future persecution is well-founded if there is a ten percent chance that the persecutor may harm the asylum-seeker on account of a protected ground in the future.[98] An individual is presumed to have a well-founded fear of future persecution if she experienced past persecution. If the asylum-seeker has not experienced past persecution, she is not eligible for the presumption and

[93] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 845–48.

[94] *See id.* at 848.

[95] *See* Daniel Susser, Beate Roessler & Helen Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, 4 GEO. L. TECH. REV. 1, 4 (2019) (arguing that "the role autonomy plays in political decision-making is more fundamental and consequential than it is in consumer decision-making").

[96] *See id.* at 9–12 (discussing the alleged voter manipulation by Cambridge Analytica).

[97] *See* U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13.

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

must prove independently that her fear of future persecution is well-founded.[99]

Regardless of whether a claim involves the offline or online realms, an individual must establish three elements to be eligible for asylum: (1) the persecutor is the asylum-seeker's government or a non-state actor whom her government is unable or unwilling to control;[100] (2) there is a connection between the harm and one or more protected grounds—that is, there is a "persecutory nexus;"[101] and (3) the asylum-seeker experienced or may experience harm amounting to persecution—that is, there is "persecutory harm."[102]

For claims involving allegations of privacy harms, establishing the first element means demonstrating one of two possible scenarios: (1) the asylum-seeker's government engaged in conduct resulting in a privacy harm rising to the level of persecution; or (2) the asylum-seeker's government was unable or unwilling to control a non-state actor engaged in such conduct.[103] An example of the first scenario would be a government that censors its citizens' communications. As an example of the second scenario, a non-state actor who steals and accumulates debt on an individual's credit card could also be a persecutor, under certain circumstances, if the government is unable or unwilling to control such conduct. As another example, a social media platform that censors its users could also be classified as a persecutor if the government is unable or unwilling to control the platform's conduct. Of course, the social media platform, or any other non-state actor, could also be classified as a government actor under the right circumstances.[104]

The second element in an asylum claim is the persecutory nexus—the connection between the harm and a protected ground.[105] A nexus is

---

[99] *See* 8 U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13.

[100] *See* 8 U.S.C. §§ 1101(a)(42); 8 C.F.R. §§ 208.13, 1208.13.

[101] *See* INS v. Elias-Zacarias, 502 U.S. 478, 481–82 (1992) (requiring a nexus between the persecutor's reasons for harming an individual and the individual's identification or association with one of the five protected grounds of asylum).

[102] *See* 8 U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13. Even after establishing eligibility for asylum, an asylum-seeker may nonetheless be barred from asylum due to her own actions or associations. Bars to asylum range from the failure to file the asylum application within one year of arrival in the United States to the prohibition against granting asylum to serious criminals, persecutors, or terrorists. *See* 8 C.F.R. §§ 208.4, 208.13, 208.14, 1208.4, 1208.13, 1208.14 (2022). Additionally, even if an individual is not otherwise barred from relief under the INA or its implementing regulations, she may be denied asylum in the exercise of discretion. *See* Kouljinski v. Keisler, 505 F.3d 534, 541–43 (6th Cir. 2007); Kalubi v. Ashcroft, 364 F.3d 1134, 1137–42 (9th Cir. 2004); Matter of Pula*,* 19 I&N Dec. 467, 471 (BIA 1987).

[103] *See* 8 U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13. This Article assumes that, in the case of an online persecutor, the persecutor's identity is known or ascertainable.

[104] The circumstances under which a social media platform may be classified as a government-sponsored or -sanctioned actor have yet to be defined—or even addressed—under U.S. asylum law. Asylum law will need to wrestle with this issue in the future. In addition, in the future, U.S. asylum law may need to determine whether an online platform is a sovereign statelike actor in it is own right, regardless of its connection to a traditional nation-state. *See* Molly K. Land, *Regulating Private Harms Online: Content Regulation under Human Rights Law*, *in* HUMAN RIGHTS IN THE AGE OF PLATFORMS 285 (Rikke Frank Jorgensen, ed. 2019) (arguing that online platforms' actions should "be seen as action by the state, since in many cases the state has expressly or implicitly imposed an obligation on these private companies to regulate speech on its behalf"); Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 199–203 (2017) (explaining how online platforms are emerging as transnational sovereigns).

[105] *See Elias-Zacarias*, 502 U.S. at 481–82 (requiring a nexus between a persecutor's reasons for harming an individual and the individual's identification or association with one of the five protected grounds of asylum).

established through evidence that the persecutor was sufficiently motivated to harm the asylum-seeker on account of one or more protected grounds. The INA provides that "at least one central reason" for harming an asylum-seeker must be due to a protected ground.[106] For example, government surveillance or censorship may be persecutory if the persecutor's motivation for these acts was to monitor or silence an individual because of her political opinion.[107] Continuing with the prior example of the theft and misuse of an individual's credit card, such an act could also be persecutory if the persecutor stole and misused the credit card to target the victim on account of her religion.

Establishing the third element of an asylum claim requires demonstrating that the harm was sufficiently severe to be classified as persecutory harm. Courts have repeatedly held that physical violence,[108] imprisonment and detention,[109] and certain economic harms may rise to the level of persecution.[110] Crucially, courts have also recognized that emotional and psychological harm, even without accompanying physical or tangible harm, may amount to persecution.[111] While certain harms are categorically classified as persecutory, other harms have been deemed sufficiently severe based on context.[112]

While Part IV will expand on how privacy harms may be severe enough to be elevated to persecutory harms, a few examples of how that may work are in order here. The following examples include material related to sexual assault, violence, and pornography. Starting with a privacy harm that

---

[106] *See* 8 U.S.C. § 1158(b)(1)(B)(i); *see also* 8 C.F.R. §§ 208.13, 1208.13; Parussimova v. Mukasey, 555 F.3d 734, 741 (9th Cir. 2009). Notably, there may still be a nexus even if a persecutor imputes—even incorrectly—a protected ground to an asylum-seeker. *See, e.g.*, Javed v. Holder, 715 F.3d 391, 393, 396–97 (1st Cir. 2013); Amanfi v. Ashcroft, 328 F.3d 719, 730 (3d Cir. 2003). Additionally, while an applicant for asylum must demonstrate that a protected ground was "at least one central reason" for the persecutor's privacy-threatening conduct, an applicant for withholding of removal may only need to show that her protected ground was "a reason" for the persecutor's conduct, which is a less demanding standard. *See* Guzman-Vazquez v. Barr, 959 F.3d 253, 270–74 (6th Cir. 2020); Barajas-Romero v. Lynch, 846 F.3d 351, 358–60 (9th Cir. 2017). *But see* Matter of C-T-L-, 25 I&N Dec. 341, 348 (BIA 2010). *See generally* 8 U.S.C. § 1231 (2022); 8 C.F.R. §§ 208.16, 1208.16 (2022) (governing the relief of withholding of removal).

[107] *See, e.g.*, Nasseri v. Moschorak, 34 F.3d 723, 730 (9th Cir. 1994) (noting that the persecutors' "surveillance of Nasseri further establishes that they believed her to be a political enemy").

[108] *See, e.g.*, Chand v. INS, 222 F.3d 1066, 1073–74 (9th Cir. 2000) ("Physical harm has consistently been treated as persecution."); *see also* Xinbing Song v. Sessions, 882 F.3d 837, 841 (9th Cir. 2017) (as amended) (recognizing torture and beatings as persecutory harm); Avendano-Hernandez v. Lynch, 800 F.3d 1072, 1079 (9th Cir. 2015) (recognizing rape and sexual assault as persecutory harm); Abebe v. Gonzales, 432 F.3d 1037, 1042 (9th Cir. 2005) (en banc) (recognizing female genital mutilation as persecutory harm).

[109] *See, e.g.*, Bondarenko v. Holder, 733 F.3d 899, 908–09 (9th Cir. 2013); Kalubi v. Ashcroft, 364 F.3d 1134, 1136 (9th Cir. 2004); Vladimirova v. Ashcroft, 377 F.3d 690, 693–96 (7th Cir. 2004).

[110] *See, e.g.*, Matter of T-Z-, 24 I&N Dec. 163, 171 (BIA 2007) (explaining that "the deliberate imposition of severe economic disadvantage or the deprivation of liberty, food, housing, employment or other essentials of life" may amount to persecution) (citation and italics omitted); *see also* Ming Dai v. Sessions, 884 F.3d 858, 870 (9th Cir. 2018) (finding that job loss may contribute to a finding of persecution), *vacated and remanded on other grounds*, Garland v. Ming Dai, 141 S.Ct. 1669 (2021); Vitug v. Holder, 723 F.3d 1056, 1065 (9th Cir. 2013) (finding that the inability to find a job may contribute to a finding of persecution); Korablina v. INS, 158 F.3d 1038, 1045 (9th Cir. 1998) (finding that job loss and obstacles to career advancement may contribute to a finding of persecution).

[111] *See, e.g.*, Mashiri v. Ashcroft, 383 F.3d 1112, 1120 (9th Cir. 2004) ("Persecution may be emotional or psychological, as well as physical.") (citations omitted); *see also* Doe v. U.S. Att'y Gen., 956 F.3d 135, 145–46 (3d Cir. 2020) (quoting *Mashiri*, 383 F.3d at 1120); Ouk v. Gonzales, 464 F.3d 108, 111 (1st Cir. 2006) ("[U]nder the right set of circumstances, a finding of past persecution might rest on a showing of psychological harm.") (quoting Makhoul v. Ashcroft, 387 F.3d 75, 80 (1st Cir. 2004)); Weerasekara v. Holder, 583 F. App'x, 795, 796 (9th Cir. 2014); Metry v. Holder, 506 F. App'x 570, 571 (9th Cir. 2013).

[112] *See, e.g.*, Jiang v. Gonzales, 485 F.3d 992, 997 (7th Cir. 2007); Guo v. Ashcroft, 361 F.3d 1194, 1203 (9th Cir. 2004).

involves an individual's bodily and physical integrity, let us assume that an individual holds an anti-government political opinion and, due to her political opinion, the mayor rapes her. Under U.S. asylum law, rape is a physical harm that has been recognized as sufficiently severe to qualify as persecution.[113] As the Ninth Circuit noted in *Kaur v. Wilkinson*, "[t]he hallmarks of persecutory conduct include, but are not limited to, the violation of bodily integrity and bodily autonomy."[114] But rape is more than just physical harm: it is also a gross *sexual privacy violation* tantamount to persecutory harm. As Citron has explained, sexual privacy violations have severe ramifications: they deny victims agency over their intimate lives, affect intimate relationships, cause visceral fear, reduce individuals to sexual objects that can be exploited and exposed, destroy individuals' identities, stigmatize individuals, cause profound emotional trauma, and affect job prospects.[115] These resulting harms could be lumped over-simplistically into the category of emotional and psychological harm, which U.S. asylum law has recognized may, by itself, qualify as persecution.[116] But, in addition to the physical battery and emotional trauma, the resulting harms from the sexual privacy violation of the rape, such as being denied agency, having intimate relationships destroyed, and being stigmatized, may *also* be severe enough to amount to persecutory harm.

Now, let us take an example from the online realm. Continuing with the prior example, consider a scenario in which the mayor posted online a deepfake sex video of the individual, in which the targeted individual's face is fraudulently inserted into real pornography.[117] While the deepfake sex video may not necessarily involve physical harm, it may result in a sexual privacy violation. The harms resulting from the sexual privacy violation, such as being objectified, as well as losing one's identity and job, may all be sufficiently severe to amount to persecutory harm under U.S. asylum law.

Before moving to the proposed frameworks for addressing privacy harms arising in asylum claims, a few additional words are necessary regarding how privacy harms in general may be elevated to persecutory harms. Significantly, courts may look to an asylum-seeker's perception of the privacy harm to determine whether to classify it as persecutory.[118] For example, in determining that a forced pregnancy examination was

---

[113] *See, e.g.*, Kaur v. Wilkinson, 986 F.3d 1216, 1222 (9th Cir. 2021) ("We have consistently treated rape as one of the most severe forms of persecution an asylum-seeker can suffer."); *Avendano-Hernandez*, 800 F.3d at 1079 (recognizing rape and sexual assault as persecutory harm); Hernandez-Montiel v. INS, 225 F.3d 1084, 1097 (9th Cir. 2000) (recognizing rape as persecutory harm), *overruled on other grounds by* Thomas v. Gonzales, 409 F.3d 1177, 1187 (9th Cir. 2005); *see also* Hernandez-Chacon v. Barr, 948 F.3d 94, 105 (2d Cir. 2020) (noting that the persecutors likely raped the asylum-seeker because of her political opinion).

[114] *Kaur*, 986 F.3d at 1222.

[115] *See* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1921–28 (2019) [hereinafter Citron, *Sexual Privacy*].

[116] *See, e.g.*, *Ouk*, 464 F.3d at 111; *Mashiri*, 383 F.3d at 1120.

[117] *See* Citron, *Sexual Privacy*, *supra* note 115, at 1921.

[118] *See, e.g.*, Ordonez-Quino v. Holder, 760 F.3d 80, 90–92 (1st Cir. 2014) (finding that a child's point of view must be considered in evaluating whether the past harm amounts to persecution); U.S. CITIZENSHIP AND IMMIGRATION SERVICES: RAIO DIRECTORATE—OFFICER TRAINING, *Definition of Persecution and Eligibility Based on Past Persecution* § 3.2.5 (Dec. 20, 2019), https://www.uscis.gov/sites/default/files/document/foia/Persecution_LP_RAIO.pdf [hereinafter USCIS PAST PERSECUTION GUIDANCE] (recommending consideration of an elderly individual's point of view when evaluating whether harm amounts to persecution).

persecutory, the Ninth Circuit in *Li v. Ashcroft* considered the asylum-seeker's perception of the exam, specifically noting that the asylum-seeker had described it as "rape-like."[119] Given that many privacy harms will be the result of novel online conduct for which there is no equivalent or analogous offline conduct, it is important to keep in mind the significance and relevance of the asylum-seeker's perception of the privacy harm. Revisiting the prior example of the deepfake sex video, it almost goes without saying that the individual's perception of the video as traumatic is critical to understanding the nature and severity of the harm.

In the case of privacy harms, an asylum-seeker's opinion or perception of the nature and severity of the harm may also depend on context.[120] For example, an individual may object to online surveillance because the information gathered about her pertains to her religion or another protected identity. She may also find the online surveillance objectionable if the information gleaned from her social media account was used to target her on account of her race, religion, or another protected ground—even if the information had nothing to do with her protected identity.[121] For example, an individual may not, in general, object to a government or social media platform collecting information about her non-religious or secular wedding ceremony, but she may find it highly objectionable if that information is used to target her on account of her religion or apostasy, collect information about her religious beliefs, *or* deny her online access because of her religious identity or lack thereof.

Additionally, as with all claims of persecution, whether or not they deal with privacy or non-privacy harms, it is important to point out that, under U.S. asylum law, an asylum-seeker's credible testimony alone—that is, her testimony without any additional corroborating evidence—may be sufficient to establish persecution.[122] Thus, returning to the deepfake sex video example, the targeted individual's testimony regarding the video's detrimental effects—and, even, the authorship and reasons behind its making—may be enough to establish persecution.

Finally, even a culturally or widely accepted practice may still amount to persecution.[123] Importantly, determining whether harm rises to the level of

---

[119] Li v. Ashcroft, 356 F.3d 1153, 1158, 1158 n.4 (9th Cir. 2004) (en banc).

[120] *See* Helen Nissenbaum, PRIVACY IN CONTEXT 2–3 (2010) (theorizing that individuals principally care about ensuring that information flows appropriately depending on norms governing distinct social contexts, such as education, health care, and politics).

[121] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (explaining that one of the special harms that can arise from surveillance is that "critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance").

[122] *See* 8 U.S.C. § 1158(b)(1)(B)(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a); Matter of Mogharrabi, 19 I&N Dec. 439, 445 (BIA 1987) ("The alien's own testimony may in some cases be the only evidence available, and it can suffice where the testimony is believable, consistent, and sufficiently detailed to provide a plausible and coherent account of the basis for his fear."); *see also Final Rule*, *supra* note 14, at 80,304 n. 29 (reiterating that an individual's testimony alone may be sufficient to meet her burden of proof with respect to an asylum claim); Korniejew v. Ashcroft, 371 F.3d 377, 382 (7th Cir. 2004) (emphasizing in dicta that it is "well-established" that the asylum-seeker's credible testimony alone may sustain an asylum claim).

[123] *See, e.g.*, Mohammed v. Gonzales, 400 F.3d 785, 796 n.15 (9th Cir. 2005) ("The fact that persecution is widespread does not alter our normal approach to determining refugee status or make a particular asylum claim less compelling…nor does its cultural acceptance.") (citation marks omitted) (quoting Ndom v. Ashcroft, 384 F.3d 743, 752 (9th Cir. 2004)).

persecution requires individualized analysis.[124] Thus, if the privacy-threatening conduct, such as online censorship or surveillance, is endemic or even just accepted by some individuals in the asylum-seeker's home country, it may still be tantamount to persecution in general and with respect to that particular asylum-seeker.

Now that the basic elements of an asylum claim have been outlined, how should asylum claims alleging privacy harms be conceptualized? The following sections will lay out three frameworks for addressing privacy harms under U.S. asylum law.

B. As Evidence of Past Persecution

One approach to privacy harms in asylum claims is to examine whether the harm is evidence of past persecution. Given the presumption of a well-founded fear of future persecution if an individual establishes past persecution, determining whether a privacy harm supports a finding of past persecution can play a critical role in an asylum adjudication.[125] Before addressing how a privacy harm may serve as evidence of past persecution, it is first necessary to understand how courts have historically made past persecution determinations.

As discussed earlier, courts have emphasized the fact-dependent nature of persecution determinations.[126] Courts have also explained that a wide variety of harms may be relevant to a persecution determination.[127] In the words of the First Circuit, "[p]ersecution is a fluid term, not defined by statute[,]" and "courts usually assess whether harm rises to the level of persecution on a case-by-case basis."[128] Significantly, courts have stressed that persecution determinations require a contextual examination of all relevant information.[129] As the Ninth Circuit has noted, a court will consider "the totality of the circumstances."[130] The Seventh Circuit has similarly explained that a court will examine "the evidence as a whole."[131]

In more concrete terms, to determine whether past persecution occurred, courts will consider the context in which the harm occurred, including the circumstances and events in an asylum-seeker's home country, as well as any other incidents of harm directed at the asylum-seeker, her family or friends, or others.[132] For instance, in *Ouda v. INS*, the Sixth Circuit found past

---

[124] *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.").

[125] *See* 8 U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13.

[126] *See, e.g.*, Cordon-Garcia v. INS, 204 F.3d 985, 991 (9th Cir. 2000) (noting that "[t]he determination that actions rise to the level of persecution is very fact-dependent") (citation omitted).

[127] *See, e.g.*, *id.* (noting that persecution covers a range of harms).

[128] *Ordonez-Quino*, 760 F.3d at 87–88.

[129] *See, e.g.*, Doe v. U.S. Att'y Gen., 956 F.3d 135, 144 (3d Cir. 2020) (discussing the significance of contextualizing a threat in making a past persecution determination); Herrera-Reyes v. U.S. Att'y Gen., 952 F.3d 101, 112 (3d Cir. 2020) (similar); Tamara-Gomez v. Gonzales, 447 F.3d 343, 348 (5th Cir. 2006) (similar).

[130] Guo v. Ashcroft, 361 F.3d 1194, 1203 (9th Cir. 2004).

[131] Jiang v. Gonzales, 485 F.3d 992, 997 (7th Cir. 2007) (citation omitted).

[132] *See, e.g.*, *Herrera-Reyes*, 952 F.3d at 112 (finding that a death threat made in a "pattern of harassment encompassing property damage, threats of violence, and actual violence" in conjunction with the murder of the asylum-seeker's political compatriot cumulatively amounted to past persecution); Krotova v. Gonzales, 416 F.3d 1080, 1087 (9th Cir. 2005) ("The combination of sustained economic pressure, physical violence and threats against the Petitioner and her close associates, and the restrictions

persecution where the asylum-seekers "personally suffered" and the evidence clearly showed "a grim picture of human rights violations in post-war Kuwait."[133] Likewise, in *Sanchez Jimenez v. U.S. Attorney General*, the Eleventh Circuit found that an asylum-seeker had experienced past persecution because the persecutors threatened and were violent towards both him and his daughter.[134] Similarly, in *Khup v. Ashcroft,* the Ninth Circuit based a finding of past persecution, in part, on the fact that a fellow preacher was arrested, tortured, and killed, thus emotionally traumatizing the asylum-seeker.[135]

In assessing whether past persecution occurred, courts will also consider the cumulative effect of individual threats and incidents of harm.[136] As the Ninth Circuit noted in *Korablina v. INS*, "[t]he key question is whether, looking at the cumulative effect of all the incidents a petitioner has suffered, the treatment she received rises to the level of persecution."[137] Sometimes, in finding that persecution has occurred, courts have focused on the repetition or aggregation of multiple threats and harms.[138] Other times, courts have highlighted that there have been multiple threats and harms over the course of many years.[139] For example, in *Baballah v. Ashcroft*, the Ninth Circuit explained that "the severity of harm is compounded when incidents of persecution have occurred on more than one occasion."[140] Even multiple threats alone—that is, without, for example, any accompanying physical or economic harms—may amount to past persecution.[141] Significantly, courts have found that threats and harms that might not individually rise to the level

on the Petitioner's ability to practice her religion cumulatively amount to [past] persecution."); Matter of O-Z- & I-Z-, 22 I&N Dec. 23, 25–26 (BIA 1998) (finding past persecution where an asylum-seeker suffered multiple beatings, repeated and personalized threats were delivered to his home, property was vandalized and destroyed, and his son was beaten, intimidated, and humiliated).

[133] Ouda v. INS, 324 F.3d 445, 453 (6th Cir. 2003) (finding past persecution in the context of human rights violations); *see also* Korablina v. INS, 158 F.3d 1038, 1045 (9th Cir. 1998) (finding past persecution in the context of political and social turmoil in the asylum-seeker's home country).

[134] *See* Sanchez Jimenez v. U.S. Att'y Gen., 492 F.3d 1223, 1233–34 (11th Cir. 2007); *see also* Mashiri v. Ashcroft, 383 F.3d 1112, 1121 (9th Cir. 2004); Navas v. INS, 217 F.3d 646, 658 (9th Cir. 2000); Sangha v. INS, 103 F.3d 1482, 1487 (9th Cir. 1997).

[135] *See* Khup v. Ashcroft, 376 F.3d 898, 904 (9th Cir. 2004).

[136] *See, e.g.*, Mejia v. U.S. Att'y Gen., 498 F.3d 1253, 1257–58 (11th Cir. 2007) (finding past persecution where the asylum-seekers experienced "the cumulative effects of the escalating threats and attacks") (citation omitted); Ahmed v. Keisler, 504 F.3d 1183, 1194 (9th Cir. 2007) (finding past persecution where an asylum-seeker experienced the cumulative effect of multiple incidents of harm over a period of years).

[137] *Korablina*, 158 F.3d at 1044.

[138] *See, e.g.*, Reyes-Guerrero v. INS, 192 F.3d 1241, 1243, 1245–46 (9th Cir. 1999) (finding past persecution where the asylum-seekers were subjected to repeated bribe attempts, personal confrontations, and death threats); *see also* Lim v. INS, 224 F.3d 929, 936 (9th Cir. 2000) ("[R]epeated and especially menacing death threats can constitute a primary part of a past persecution claim . . . .") (citations omitted).

[139] *See, e.g.*, *Ahmed*, 504 F.3d at 1194 ("Where an asylum applicant suffers such harm on more than one occasion, and, as in this case, is victimized at different times over a period of years, the cumulative effect of the harms is severe enough that no reasonable fact-finder could conclude that it did not rise to the level of persecution.") (citing Chand v. INS, 222 F.3d 1066, 1074 (9th Cir. 2000) (Reinhardt, J.)); *Mejia*, 498 F.3d at 1257–58 (finding past persecution where harm occurred over an eighteen-month period); *see also* Carreto-Escobar v. Barr, 810 F. App'x 521, 524 (9th Cir. 2020) (finding past persecution where harm occurred "over a period of years").

[140] Baballah v. Ashcroft, 367 F.3d 1067, 1076 (9th Cir. 2003) (citation and quotation marks omitted).

[141] *See, e.g.*, Bedoya v. Barr, 981 F.3d 240, 247 (4th Cir. 2020) (finding that threats alone amount to past persecution); Crespin-Valladares v. Holder, 632 F.3d 117, 126–27 (4th Cir. 2011) (finding that three death threats amount to past persecution); *see also* Thomas v. Ashcroft, 359 F.3d 1169, 1179 (9th Cir. 2004) (noting that "threats of violence and death are enough" to establish past persecution) (citation omitted).

of past persecution may, taken together, amount to persecution.[142] Courts have also considered the cumulative effects of escalating threats and harms,[143] looking to whether the "overall trajectory" of the individual threats and incidents of harms amounts to persecution.[144] In making a cumulative analysis—regardless of the number of threats or harms or over how many years—courts often emphasize evaluating the *impact* of those cumulative threats or harms.[145]

It is important to point out that this approach to contextualizing past harms mirrors the emphasis on context in the privacy law sphere,[146] including the recognition that many privacy harms—even small or seemingly insignificant ones—may cumulatively or overall amount to a greater harm.[147] As Citron and Solove note outside the context of asylum law, "[f]or many privacy harms, the injury may appear small when viewed in isolation . . . [b]ut when done by hundreds or thousands of companies, the harm adds up."[148]

So, then, how might a privacy harm be evidence of past persecution? In short, a privacy harm in the context of other threats, harms, or events may be evidence of past persecution. In this regard, the privacy harm is additional evidence supporting or corroborating a finding of past persecution. In other words, a privacy harm may contribute to a finding of cumulative or overall past persecution.[149] For example, under this approach, online censorship that occurs in the context of political unrest and has a chilling effect on an asylum-seeker's political participation may amount to past persecution. As another example, being abducted, threatened, and then surveilled online may

[142] *See* Delgado v. U.S. Att'y Gen., 487 F.3d 855, 861–62 (11th Cir. 2007) ("Although each of the incidents taken separately would not establish persecution . . . when considered together the events compel the conclusion that [the asylum-seekers] suffered past persecution due to their political opinions."); Singh v. INS, 94 F.3d 1353, 1358–59 (9th Cir. 1996) ("While a single incident in some cases may not rise to the level of persecution, the cumulative effect of several incidents may constitute persecution.") (citation omitted).

[143] *See, e.g.*, Mejia v. U.S. Att'y Gen., 498 F.3d 1253, 1257–58 (11th Cir. 2007) (finding past persecution where an asylum-seeker and his wife experienced "the cumulative effects of the escalating threats and attacks") (citation omitted); Nakibuka v. Gonzales, 421 F.3d 473, 477–78 (7th Cir. 2005) (finding past persecution where, following incidents of detention, physical assault, and attempted rape, an asylum-seeker and her family were subjected to escalating threats of harm).

[144] *See, e.g.*, Gomez-Zuluaga v. U.S. Att'y Gen., 527 F.3d 330, 343 (3d Cir. 2008) (finding that, given "[t]he overall trajectory of the harassment against [the asylum-seeker] continued and escalated with each new incident[,]" the asylum-seeker's abduction amounted to persecutory harm) (citations omitted).

[145] *See Mejia*, 498 F.3d at 1257–58 (finding that, while each instance of harm was not individually persecutory, the court was "required to consider the *cumulative* impact of the mistreatment the petitioners suffered") (emphasis in the original) (citation omitted); *see also* Rempell, *supra* note 9, at 288 ("[M]ere aggregation overlooks the context of the events in a manner that can skew the true extent of harm."). There have been, of course, significant, historical instances when, to the detriment of the asylum-seeker, courts have discounted the context in which the harms occurred. *See, e.g.*, Marouf, *Sexual and Reproductive Harm*, supra note 33, at 85–86, 165.

[146] *See, e.g.*, Citron & Solove, *Privacy Harms*, *supra* note 6, at 818 ("Privacy harms are highly contextual, with the harm depending upon how the data is used, what data is involved, and how the data might be combined with other data.").

[147] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397 (2000) (explaining, in the context of consumers, how the collection of small bits of data—including data voluntarily provided—may have cumulative injurious effects).

[148] Citron & Solove, *Privacy Harms*, *supra* note 6, at 797.

[149] *See, e.g.*, Manzur v. U.S. Dep't of Homeland Sec., 494 F.3d 281, 292–93 (2d Cir. 2007) (finding that surveillance amounted to past persecution).

overall amount to persecution.[150] Finally, returning to the persecutorial mayor hypothetical, if, in addition to the deepfake sex video, which invaded the asylum-seeker's privacy and emotionally traumatized her, the mayor also had the asylum-seeker's cousin arrested, those experiences may rise to the level of past persecution.

But what if the asylum-seeker's past experiences do *not* amount to past persecution? Can a privacy harm be evidence of future persecution? Answering this question will be the focus of the next section.

C. AS EVIDENCE PREDICTING FUTURE PERSECUTION

To be eligible for asylum, an individual must have a well-founded fear of future persecution.[151] While an individual who has experienced past persecution is presumed to have a well-founded fear of future persecution, an individual may independently establish that her fear is well-founded.[152] An asylum-seeker's fear of future persecution is well-founded if the likelihood of future persecution is "objectively reasonable."[153] The U.S. Supreme Court has held that this likelihood is objectively reasonable if there is a ten percent chance that the persecutor may harm the asylum-seeker on account of a protected ground in the future.[154] In the absence of past persecution, an asylum-seeker may establish this ten percent likelihood of future persecution through two routes.[155] One route is to present evidence that she would be targeted or singled out for future persecution.[156] Alternatively, as a second route, an asylum-seeker may prove that her fear is well-founded by presenting evidence that there is a "pattern or practice" in her country of persecution of a group of persons "similarly situated."[157]

Privacy-threatening conduct may be evidence of future persecution. If the privacy-threatening conduct is evidence of past persecution, it may support a finding that the individual warrants the presumption of future persecution.[158] Alternatively, even if the past privacy-threatening conduct does not rise to the level of persecution, it may still serve as evidence that the asylum-seeker will be persecuted in the future.[159] Even a privacy harm

---

[150] *Cf.* Gomez-Zuluaga v. U.S. Att'y Gen., 527 F.3d 330, 342–43 (3d Cir. 2008) (finding that an asylum-seeker's eight-day abduction amounted to persecution "in the context" of in-person surveillance and threats).

[151] *See* 8 U.S.C. §§ 1101(a)(42), 1158; 8 C.F.R. §§ 208.13, 1208.13.

[152] *See id.*

[153] *See* INS v. Cardoza-Fonseca, 480 U.S. 421, 440 (1987). In addition to proving that her fear is objectively reasonable, an asylum-seeker must also prove that her fear is subjectively genuine. *See id.* at 430–31. To do so, the asylum-seeker must testify credibly that she fears being persecuted in the future. *See, e.g.*, Parada v. Sessions, 902 F.3d 901, 909 (9th Cir. 2018); *cf.* Li Tao v. Sessions, 717 F. App'x 65, 67 (2d Cir. 2018) (holding that the asylum-seeker's testimony and evidence of her online political presence established her subjective fear of future persecution but not the objective reasonable possibility that she would be singled out for future persecution).

[154] *Cardoza-Fonseca*, 480 U.S. at 440; *see also* 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."); Al-Harbi v. INS, 242 F.3d 882, 888 (9th Cir. 2001) ("[E]ven a ten percent chance of persecution may establish a well-founded fear.").

[155] *See* 8 C.F.R. §§ 208.13(b)(2)(iii), 1208.13(b)(2)(iii); *see also* Wakkary v. Holder, 558 F.3d 1049, 1060 (9th Cir. 2009) (explaining the two regulatory routes).

[156] *See* 8 C.F.R. §§ 208.13(b)(2)(iii), 1208.13(b)(2)(iii).

[157] *See id.*

[158] *See id.*

[159] *See id.*

that occurs *after* the asylum-seeker has left her home country may indicate that there is a likelihood of future persecution.[160]

Online surveillance is a good example of how privacy-threatening conduct can be evidence of future persecution. To begin with, online surveillance may be evidence of the persecutor's interest in targeting or singling out the asylum-seeker for future harm.[161] If, for example, an individual is a member of an anti-government dissident group, the government may monitor her Twitter feed "to obtain more information about the political activities of someone [it] believed to be a political enemy" or "to obtain evidence against her."[162] Online surveillance *directed at others* may also serve as evidence of future persecution.[163] For example, if there is a pattern or practice of the government surveilling family members, co-religionists, or fellow dissidents on messaging apps, such as WeChat or WhatsApp, this may be evidence that the asylum-seeker—who shares a familial relationship, religion, or political view with those surveilled—could also be targeted in the future either online or offline.[164]

In addition to serving as evidence of the persecutor's interest in harming the asylum-seeker or similarly situated individuals in the future, online surveillance may also be used as a *tool* to facilitate future offline or online persecution. The act of spying on an individual online and gathering data about her may invade her personhood and peace of mind.[165] But online surveillance may also reveal information about an asylum-seeker's whereabouts, online communications, and online and offline associations that may lead to concrete offline ramifications.[166] Through online surveillance, a persecutor may become aware of an individual's race, religion, or other protected identity, catalyzing or furthering his interest in

[160] *See id.* Under the regulations, only harm in an asylum-seeker's home country or country of last habitual residence may be considered past persecution. *See* 8 C.F.R. §§ 208.13(b)(1), 1208.13(b)(1). If the privacy violation occurred while the asylum-seeker was in the United States or a third country, it may serve, however, as evidence of future persecution. *See id; see, e.g.*, Kyaw Zwar Tun v. INS, 445 F.3d 554, 569–71 (2d Cir. 2006) (citing evidence that the Burmese government surveils dissidents in the United States and finding that post-flight surveillance of an asylum-seeker is evidence of future persecution); Zhang v. Ashcroft, 388 F.3d 713, 718 (9th Cir. 2004) (finding, in a withholding of removal case, that post-flight surveillance of an asylum-seeker's family remaining in his home country is indicative of future harm).

[161] *See, e.g.*, Nasseri v. Moschorak, 34 F.3d 723, 730 (9th Cir. 1994) (finding that surveillance, along with the abduction and torture of an asylum-seeker, compels a finding that the asylum-seeker's persecutors intend to harm her if she were to return to her home country); *see also* Tagaga v. INS, 228 F.3d 1030, 1034 (9th Cir. 2000).

[162] *Nasseri*, 34 F.3d at 727 (providing reasons that the persecutors may have engaged in in-person surveillance of an asylum-seeker).

[163] *See, e.g.*, Ayele v. Holder, 564 F.3d 862, 871–72 (7th Cir. 2009); Zhao v. Mukasey, 540 F.3d 1027, 1030–31 (9th Cir. 2008).

[164] *See, e.g.*, *Zhang*, 388 F.3d at 718 (finding that the "constant surveillance" of an asylum-seeker's similarly situated parents is "highly indicative" of the persecution that the asylum-seeker would experience if he were to return to his home country).

[165] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 853 ("Losing control over our personal data constitutes an injury to our peace of mind and our ability to manage risk.").

[166] *See, e.g.*, Hum. Rts. Council, *supra* note 2, ¶1 (expressing concern that online surveillance has led to "arbitrary detention, sometimes to torture and possibly to extrajudicial killings"). *Cf.* Romero v. U.S. Att'y Gen., 972 F.3d 334, 339 (3d Cir. 2020) (denying, on other grounds, a request for protection under the United Nations Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment ("CAT") in which an individual alleged that his persecutor may discover through Facebook if he were to return to his home country).

harming her offline because of that identity.[167] Additionally, the persecutor may use information gathered through surveillance but unrelated to the asylum-seeker's protected identity, or even the ostensible reason for the surveillance, to prosecute, blackmail, or otherwise harm the asylum-seeker.[168]

Finally, it should be noted that technology currently exists for discovering an individual's online presence and ascertaining her beliefs, opinions, identities, or group associations through that online presence.[169] Despite the development of such technology, multiple courts have been reluctant to recognize the ability or willingness of a persecutor to discover an individual's online presence and her connection to a protected ground and then persecute or otherwise harm her on account of that protected ground.[170] Given this judicial reluctance, it must be reiterated that to be eligible for asylum, an individual only needs to present evidence that there is a *ten percent* chance of future persecution.[171] In other words, the asylum-seeker only needs to prove that there is a possibility—but neither a certainty nor probability—of future persecution.[172]

D. AS PERSECUTION BY ITSELF

Although a privacy harm may be evidence of past or future persecution, what happens if the privacy harm is the main or only harm experienced or threatened? Can a privacy harm *by itself* amount to persecution? The short answer is yes. If one central reason behind the privacy harm involved a protected ground and the privacy harm is or was sufficiently severe, then it may amount to persecution, even if it is not accompanied by additional harms, threats, acts, or events. There are at least two ways to elevate a privacy harm to persecution by itself.

One way is to map the privacy harm onto an equivalent or analogous non-privacy harm that is also classified as persecutory.[173] For example,

---

[167] *See, e.g.*, Mirko Lai, Allesandra Teresa Cignarella, Delia Irazu Hernandez Farias, Cristina Bosco, Viviana Patti & Paolo Rosso, *Multilingual Stance Detection in Social Media Political Debates*, 63 COMPUT. SPEECH & LANGUAGE 1, 1–5 (2020) (describing a process for identifying topics and opinions on social media); Noura Farra, Cross-Lingual and Low-Resource Sentiment Analysis 1–6, 8–10, 219–23 (2019) (Ph.D. dissertation, Columbia University), https://doi.org/10.7916/d8-x3b7-1r92 (describing a process for identifying opinions from Arabic and Chinese on social media). *Cf.* Uzodinma v. Barr, 951 F.3d 960, 965 (8th Cir. 2020) (finding harmless error in the Board's reversal of an immigration judge's determination that the Nigerian government is aware, or could become aware, of an asylum-seeker's political opinions from his social media posts).

[168] *See* Richards, *supra* note 121, at 1935; *see, e.g.*, Nasseri v. Moschorak, 34 F.3d 723, 727 (9th Cir. 1994).

[169] *See, e.g.*, Lai et al., *supra* note 167, at 1–5; Farra, *supra* note 167, at 1–6, 8–10, 219–23; s*ee also* SHAHBAZ & FUNK, *Social Media Surveillance*, *supra* note 4.

[170] *See, e.g.*, Yi Lun Wang v. Garland, No. 19-2643 NAC *3–4, 7–8 (2d Cir. May 6, 2021); Ri Qiu Wang v. Barr, 794 F. App'x 52, 54 (2d Cir. 2019); Yongqing Shao v. U.S. Att'y Gen., 560 F. App'x 160, 161 (3d Cir. 2014); Y.C. v. Holder, 741 F.3d 324, 328, 333–38 (2d Cir. 2013); Toshev v. Holder, 407 F. App'x 674, 675 (4th Cir. 2011); Makhoul v. Ashcroft, 387 F.3d 75, 78–79, 81–82 (1st Cir. 2004). *Cf.* Haifeng Huang v. Garland, No. 20-72451 *3–4 n.4 (9th Cir. June 22, 2021); Ali Ben Mohamed Hendaoui v. Garland, No. 19-72873 *3 (9th Cir. Sept. 16, 2021). *But see* Mei Qin Zheng v. Holder, 538 F. App'x 51, 54 (2d Cir. 2013).

[171] *See* INS v. Cardoza-Fonseca, 480 U.S. 421, 440 (1987) (requiring only a ten percent likelihood of future persecution).

[172] *See, e.g.*, 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.").

[173] *See* Jarvis Cooper*, supra* note 5, at 782–83.

courts have found that economic or financial harms may be sufficiently severe to amount to persecutory harm.[174] Similarly, courts have recognized that emotional and psychological harm by itself may amount to persecution.[175] Thus, if the result of the privacy-threatening conduct is economic, financial, emotional, or psychological, the asylum-seeker may have experienced an injury or repercussion that is severe enough to be classified as persecutory. If one central reason that the persecutor committed or threatened the privacy harm was the asylum-seeker's actual or imputed protected ground, then the privacy-threatening or -violative conduct may amount to persecution.[176]

A second way to conceptualize privacy harms as persecutory is to acknowledge that there are some privacy harms that are severe enough to qualify as persecution even if they do not map onto a category of harms already recognized as persecutory under U.S. asylum law. Under this approach, certain privacy harms, such as lack of control harms, chilling effect harms, and manipulation harms, may be sufficiently severe *by themselves* to rise to the level of persecution. This approach would align with the U.S. courts' and government's historical openness to recognizing the novel ways that individuals may be persecuted.[177] Moreover, this approach echoes Citron and Solove's argument that there are some types of privacy harms that should be "enough" to be recognized as warranting relief or remedy.[178]

This approach also recognizes that while courts and adjudicators may invoke precedent to justify a persecution determination, their decision declaring a particular harm qualifies as persecution is essentially a *normative* judgment that the harm is unjustified and severe "enough" and the individual seeking asylum is worthy of protection.[179] In other words, a court, adjudicator, or agency's decision that a certain privacy harm, such as the loss of control over one's data, is—or is not—a persecutory harm may be based as much on precedent as on American culture and values. Naturally, to establish that the privacy harm by itself amounts to persecution, an asylum-seeker will still need to meet any necessary evidentiary burdens, as well as establish her credibility, just as she would with a non-privacy-related or

---

[174] *See, e.g.*, Matter of T-Z-, 24 I&N Dec. 163, 171 (BIA 2007) (explaining that "the deliberate imposition of severe economic disadvantage or the deprivation of liberty, food, housing, employment or other essentials of life" may amount to persecution) (citation and italics omitted); *see also* Ming Dai v. Sessions, 884 F.3d 858, 870 (9th Cir. 2018), *vacated and remanded on other grounds*, Garland v. Ming Dai, 141 S.Ct. 1669 (2021); Vitug v. Holder, 723 F.3d 1056, 1065 (9th Cir. 2013); Korablina v. INS, 158 F.3d 1038, 1045 (9th Cir. 1998).

[175] *See, e.g.*, Mashiri v. Ashcroft, 383 F.3d 1112, 1120 (9th Cir. 2004) ("Persecution may be emotional or psychological, as well as physical.") (citations omitted); *see also* Doe v. U.S. Att'y Gen., 956 F.3d 135, 145–46 (3d Cir. 2020); Ouk v. Gonzales, 464 F.3d 108, 111 (1st Cir. 2006); Weerasekara v. Holder, 583 F. App'x, 795, 796 (9th Cir. 2014); Metry v. Holder, 506 F. App'x 570, 571 (9th Cir. 2013).

[176] *See* INS v. Elias-Zacarias, 502 U.S. 478, 481–82 (1992) (requiring a nexus between a persecutor's reasons for harming an individual and the individual's identification or association with one of the five protected grounds of asylum); *see also* 8 U.S.C. § 1158(b)(1)(B)(i) (requiring that "at least one central reason" for harming an asylum-seeker must be due to a protected ground); 8 C.F.R. §§ 208.13, 1208.13; Parussimova v. Mukasey, 555 F.3d 734, 741 (9th Cir. 2009) (applying this statutory requirement).

[177] *See* discussion *supra* Section II.A.

[178] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 854.

[179] *See* T. Alexander Aleinikoff, *The Meaning of "Persecution" in United States Asylum Law*, 3 INT'L J. REFUGEE L. 5, 12–13, 27 (1991) (explaining that to determine whether a harm amounts to persecution is to make a normative judgment about the justification for the harm and the degree of the harm's severity).

offline harm or injury.[180] There is, however, no legal, conceptual, or moral reason to exclude categorically a privacy harm as persecution by itself.

E. AS ONLINE PERSECUTION

What if, in addition to being the main or only harm, a privacy harm's origins or effects are principally online? Could an online privacy harm *by itself* amount to persecution? Given that there is likely to be an uptick in asylum claims alleging online privacy harms as internet use increases over time,[181] answering this question is critical. Recognizing that an online privacy harm may by itself amount to persecution requires several assumptions. To begin with, this means assuming that there are certain harms—whether or not they are privacy-related—that could be sufficiently severe even if their origins or effects are in the online realm.[182] Next, it means acknowledging that an online privacy harm may be sufficiently severe even if there are no concomitant offline or online harms, threats, acts, or events.[183] Additionally, an online privacy harm may be sufficiently severe even if it is novel or does not readily map onto a previously recognized persecutory harm. There may be circumstances in which some or all these assumptions are true.

Under which circumstances, then, could an online privacy harm be evidence of or amount to online persecution? As noted earlier, I define online persecution as online conduct, manipulation, threats, words, or acts that are on account of a protected ground under U.S. asylum law and have resulted or may result in a sufficiently severe injury.[184] By extension, privacy-threatening online conduct that is on account of a protected ground under U.S. asylum law and has resulted or may result in a sufficiently severe injury may amount to online persecution. In this context, the sufficiently severe injury could be one of the privacy harms categorized by Citron and Solove.

To elaborate, there are two ways to conceptualize online privacy harms as online persecution. Under the first conceptualization, if the online privacy harm can be mapped onto a cognizable harm under U.S. asylum law, then the online privacy harm may amount to online persecution. In other words, if the online conduct violates or offends an individual's privacy, resulting in economic, financial, emotional, or psychological harm, the resulting privacy harm could potentially be classified as persecutory harm *by itself*. Assuming that one central reason for the online conduct was an asylum-seeker's protected ground, then the conduct may amount to online persecution. For example, if a persecutor surveilled or censored an individual's online presence because of her identification with a protected ground, causing her to suffer privacy-related economic, financial, emotional, or psychological harm, then she may have experienced online persecution.

Under the second conceptualization, an online privacy harm that does not necessarily map onto a previously recognized persecutory harm may

---

[180] *See* 8 U.S.C. § 1158(b)(1)(B)(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a); Matter of Mogharrabi, 19 I&N Dec. 439, 445 (BIA 1987).

[181] *See* SHAHBAZ & FUNK, *Social Media Surveillance*, *supra* note 4.

[182] *See* Jarvis Cooper, *supra* note 5, at 778–79, 782.

[183] *See id.* at 782.

[184] *See* discussion *supra* Section II.A.

nonetheless amount to online persecution if it is sufficiently severe and a central reason for the privacy-threatening online conduct was an asylum-seeker's protected ground. For example, let us imagine that a persecutor has dumped information about an individual's apostasy online. An individual may experience severe emotional trauma from the doxing—the non-consensual posting of private or personally identifying information online[185]—because the content has been widely disseminated, is easily searchable, and may potentially be permanent.[186] In addition to emotional trauma, the individual may also have experienced the privacy harm of lack or loss of control over her data. This lack of control privacy harm may be sufficiently severe even without any accompanying offline harms, words, acts, or events. The injury in this scenario is that the individual lacks or has lost control over the extent to which information pertaining to her religious beliefs or apostasy is circulated online. Such harm may, in certain circumstances, be "enough" to rise to the level of persecutory harm.[187] Assuming that the persecutor engaged in the doxing in response to the asylum-seeker's religious identity, then the asylum-seeker may have experienced online persecution.

IV. ADDRESSING SPECIFIC PRIVACY HARMS UNDER U.S. ASYLUM LAW

Now that a blueprint for addressing privacy harms has been presented, this Article will turn to specific privacy harms that may be alleged in future asylum claims. Economic and psychological privacy harms can be readily addressed by existing U.S. asylum precedents. Other privacy harms—including lack of control, chilling effect, and manipulation harms—may require flexibility and openness in applying existing precedents and issuing new ones. The next sections will focus on providing examples of how these harms may arise in asylum claims and suggest how the law may address such harms in asylum adjudications. As will be shown, there will be times when privacy-threatening conduct, by itself, is a persecutory harm. At other times, the privacy-threatening conduct may involve persecutory harms downstream.[188] The discussion that follows will focus on online privacy harms.

A. ECONOMIC HARMS

As discussed in Part II, certain conduct may threaten an individual's privacy, leading to economic or financial injuries. The classic example outside the context of asylum law is identity theft.[189] Just as they do in other

[185] *See* C.S-W., *What doxxing is, and why it matters,* THE ECONOMIST (Mar. 10, 2014), https://www.economist.com/the-economist-explains/2014/03/10/what-doxxing-is-and-why-it-matters (defining "doxing," also known as "doxxing").

[186] *See* Jarvis Cooper, *supra* note 5, at 767–68, 786.

[187] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 854 (arguing, with respect to lack of control harms, that the harm—the undermining of control over the extent to which personal information is circulated—should be "enough" to be acknowledged as a harm warranting relief or remedy).

[188] *See id.* at 853 ("Privacy laws seek to regulate data flows to protect individuals from potential downstream uses.").

[189] *See id.* at 834–35.

contexts, economic privacy harms are likely to arise in future asylum claims, especially in the online realm.

In lay terms, "asylum" is often thought of as individuals seeking refuge because a regime has targeted them for their *political* or *religious* views. Americans might think of refuseniks fleeing the Soviet Union or Puritans fleeing England. In those scenarios, the harm is seen as the suppression of an individual's political or religious beliefs. U.S. asylum law goes beyond political and religious harms, specifically recognizing that an individual may experience persecutory harm that is economic or financial in nature.[190] While under U.S. asylum law the reason behind the persecutor's conduct must be an individual's race, religion, political opinion, or another protected ground, the harm itself may be economic or financial.[191]

Thus, under U.S. asylum law, economic and financial harms may amount to persecutory harms. As the Board has explained, "the deliberate imposition of severe economic disadvantage or the deprivation of liberty, food, housing, employment or other essentials of life" may amount to persecution.[192] For instance, the Ninth Circuit has identified the loss of job opportunities and obstacles to career advancement as potentially persecutory harms.[193] Economic or financial harms may even amount to persecution in the absence of other harms.[194]

It is important to point out that U.S. asylum law recognizes that a persecutor may have more than one reason for targeting an individual. So long as "at least one central reason" behind the harm is due to the asylum-seeker's protected ground, persecution may exist even if a persecutor has additional motives to harm an asylum-seeker.[195] Thus, while a persecutor may target an individual economically or financially for personal gain, he may also target the individual because of her protected identity, such as her race, religion, or political opinion.[196]

Although there are no published asylum decisions addressing economic privacy harms, applying asylum precedents to such harms is relatively straightforward. In short, if the privacy-threatening online conduct leads to immediate or downstream severe economic or financial injuries, then it may amount to persecution.

How, then, may economic privacy harms arise in asylum claims? It is easy to imagine scenarios in which privacy-threatening online conduct may lead to severe economic or financial injuries. For example, a persecutor may

---

[190] *See* Matter of T-Z-, 24 I&N Dec. 163, 170–75 (BIA 2007).

[191] *See* INS v. Elias-Zacarias, 502 U.S. 478, 481–82 (1992) (requiring a nexus between a persecutor's reasons for harming an individual and one of the five protected grounds for asylum).

[192] Matter of T-Z-, 24 I&N Dec. at 171 (citation and italics omitted).

[193] *See, e.g.*, Ming Dai v. Sessions, 884 F.3d 858, 870 (9th Cir. 2018) (finding that job loss may contribute to a finding of persecution), *vacated and remanded on other grounds*, Garland v. Ming Dai, 141 S.Ct. 1669 (2021); Vitug v. Holder, 723 F.3d 1056, 1065 (9th Cir. 2013) (finding that the inability to find a job may contribute to a finding of persecution); Korablina v. INS, 158 F.3d 1038, 1045 (9th Cir. 1998) (finding that job loss and obstacles to career advancement may contribute to a finding of persecution).

[194] *See* Matter of T-Z-, 24 I&N Dec. at 170–75.

[195] 8 U.S.C. § 1158(b)(1)(B)(i) (requiring that "at least one central reason" for harming the asylum-seeker must be due to a protected ground); 8 C.F.R. §§ 208.13, 1208.13; Parussimova v. Mukasey, 555 F.3d 734, 741 (9th Cir. 2009) (applying this statutory requirement).

[196] *See, e.g.*, Jahed v. INS, 356 F.3d 991, 999 (9th Cir. 2004) (holding that, while a persecutor was motivated to extort the targeted individual for his own financial gain, "his motive in doing so was inextricably intertwined" with the targeted individual's past political affiliation).

surveil and control an asylum-seeker's financial transactions online through his influence or authority over online transactions or digital currencies.[197] Another way in which a persecutor may harm an individual economically or financially is through online identity theft. Although the persecutor may engage in such conduct for financial gain, he may also target the individual because of her protected identity, elevating such conduct to persecution.[198]

Privacy-threatening online conduct may also lead to economic or financial harms downstream. While a persecutor may directly engage in online economic or financial harms, he may also influence others to do so. For example, the persecutor may dump the targeted individual's financial information online to encourage third parties to commit identity theft, resulting in economic or financial harm to the targeted individual.[199] Even if the doxing does not reveal financial information about the targeted individual, it may reveal other personal details about the targeted individual, such as her involvement in a political opposition party or dissident group. As a result of such "unmasking" or outing of her political involvement or opinions,[200] others may target the doxed individual economically or financially. Due to such privacy-threatening conduct, the targeted individual may lose her job, experience obstacles to career advancement, or suffer business losses.[201] Thus, privacy-threatening conduct resulting in economic or financial harms may amount to persecution.

B. EMOTIONAL AND PSYCHOLOGICAL HARMS

Privacy-threatening conduct resulting in emotional or psychological harms may amount to persecution.[202] As Citron has chronicled in her work, privacy-threatening conduct outside the context of asylum can lead to profound emotional and psychological harms.[203] Online conduct, such as

---

[197] *See, e.g.*, Maya Wang, *China's Techno-Authoritarianism Has Gone Global*, FOREIGN AFF. (Apr. 8, 2021), https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global (reporting that the Chinese banking system is adopting a digital currency, which will allow the government to surveil—and control—people's financial transactions).

[198] *See, e.g.*, Sanchez Jimenez v. U.S. Att'y Gen., 492 F.3d 1223, 1232–33 (11th Cir. 2007) (holding that persecution may exist even where a persecutor has mixed motives for harming an asylum-seeker).

[199] *See* Peter Snyder, Periwinkle Doerfler, Chris Kanich & Damon McCoy, *Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing*, PROCEEDINGS OF INTERNET MEASUREMENT CONFERENCE 437–38 (2017), https://doi.org/10.1145/3131365.3131385 (documenting that doxing frequently reveals identifying information about an individual, including financial information).

[200] *See* Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2461–62 (2017) (describing how online actors "unmask"—expose the identity of—fellow hackers for malicious and political purposes).

[201] *See, e.g.*, Emma Grey Ellis, *Whatever Your Side, Doxing is a Perilous Form of Justice*, WIRED (Aug. 17, 2017) https://www.wired.com/story/doxing-charlottesville (reporting that individuals lost their jobs after being doxed online).

[202] While Citron and Solove place such privacy harms under the umbrella of "psychological harm" with the subtypes of "emotional distress" and "disturbance," they note that these harms can encompass a range of negative mental responses and a wide array of feelings. *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 842. Along these lines, it is important to point out that U.S. asylum law does not require that an individual establish emotional or psychological harm through a medical or psychiatric evaluation. *See* 8 U.S.C. § 1158(b)(1)(B)(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a); Matter of Mogharrabi, 19 I&N Dec. 439, 445 (BIA 1987) (providing that an asylum-seeker's credible testimony alone may be sufficient to establish persecution). As such, this Article categorizes all such privacy harms as "emotional and psychological harms" in order to capture the wide range of emotional injuries that an asylum-seeker may experience as a result of past or future persecution.

[203] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 841–42; DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 4 (2014) [hereinafter CITRON, HATE CRIMES IN CYBERSPACE].

impersonation, posting nude photos, doxing, and threats, all can conjure deep fears and emotional distress that may "impede someone's life as much as certain physical injuries."[204] Similarly, identity theft can cause emotional trauma.[205]

U.S. asylum law specifically recognizes that emotional and psychological harm may contribute to a finding of persecution.[206] A court may find persecution where an asylum-seeker experienced emotional trauma due to events or harms that she personally experienced.[207] A court may also find persecution where the asylum-seeker suffered emotionally due to events or harms directed at her family or friends, or others.[208]

U.S. asylum law also recognizes that emotional and psychological harm may amount to persecutory harm even without any accompanying physical, tangible, economic, or financial harms.[209] It is important to note that this recognition that emotional trauma *alone* may amount to persecutory harm goes beyond just judicial interpretation: the U.S. Citizenship and Immigration Services has specifically issued policy guidance noting that "[p]sychological harm alone may rise to the level of persecution."[210] In this way, U.S. asylum law resembles the law of privacy torts in that both recognize that emotional and psychological harms may be the sole injury forming the basis for a claim.[211]

While courts have yet to address the issue, privacy-threatening online conduct that results in emotional and psychological harm can easily be mapped onto existing U.S. asylum precedents. Simply put, if the privacy-threatening online conduct results in emotional or psychological harm and a central reason behind the conduct was a protected ground, that may be enough to support a finding of persecution.

In future asylum claims, individuals are likely to allege severe emotional and psychological trauma emanating from privacy-threatening conduct, especially in the online realm. For example, an asylum-seeker may allege that she suffered emotionally or psychologically because she was doxed.[212] As another example, she may allege that she is emotionally traumatized by revenge pornography—the online distribution of nude photographs or other sexual imagery without the subject's consent.[213] She may similarly be

---

[204] Citron & Solove, *Privacy Harms*, *supra* note 6, at 841–42.

[205] *See id.* at 842.

[206] *See, e.g.*, Ouk v. Gonzales, 464 F.3d 108, 111 (1st Cir. 2006) (recognizing that "a finding of past persecution might rest on a showing of psychological harm") (citation omitted); Mashiri v. Ashcroft, 383 F.3d 1112, 1120 (9th Cir. 2004) (recognizing that "[p]ersecution may be emotional or psychological") (citations omitted).

[207] *See, e.g.*, Hernandez-Montiel v. INS, 225 F.3d 1084, 1097–98 (9th Cir. 2000) (finding past persecution where the asylum-seeker was raped, resulting in emotional trauma), *overruled on other grounds by* Thomas v. Gonzales, 409 F.3d 1177, 1187 (9th Cir. 2005).

[208] *See, e.g.*, Khup v. Ashcroft, 376 F.3d 898, 904 (9th Cir. 2004) (finding past persecution where an asylum-seeker was emotionally traumatized due to the arrest, torture, and killing of a fellow preacher).

[209] *See, e.g.*, *Ouk*, 464 F.3d at 111; *Mashiri*, 383 F.3d at 1120; s*ee also* Weerasekara v. Holder, 583 F. App'x, 795, 796 (9th Cir. 2014); Metry v. Holder, 506 F. App'x 570, 571 (9th Cir. 2013).

[210] USCIS PAST PERSECUTION GUIDANCE, *supra* note 118, § 3.7.1.

[211] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 843.

[212] *See* MacAllister, *supra* note 200, at 2452–61 (documenting the emotional harm from doxing).

[213] *See* Drew Harwell, *Fake-porn videos are being weaponized to harass and humiliate women: 'Everybody is a potential target'*, WASH. POST (Dec. 30, 2018), https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target (defining revenge porn and documenting the emotional trauma of Rana Ayyub, an investigative journalist in India who was subjected to a deepfake pornographic video of her).

emotionally scarred by being the subject of an online deepfake.[214] Her emotional trauma may be heightened if the deepfake incorrectly attributes a belief, opinion, or action to her, such as attending a political rally or religious ceremony.[215] An asylum-seeker may also allege that she has suffered psychologically because she was surveilled or censored online. Her emotional or psychological trauma may stem from the anxiety or embarrassment of believing that she is or will be watched or monitored.[216] An individual's emotional trauma from being watched may be exacerbated if she believes that she is being watched *because* of her beliefs, opinions, or identity.[217] Her anxiety may be further compounded by the anticipation that the persecutor's online conduct may lead to additional online or offline harms.[218] Thus, privacy-threatening conduct that causes emotional or psychological harms is likely to be alleged and can be easily addressed in future asylum claims.

C. LACK OF CONTROL

A unique privacy harm that may appear in future asylum claims is one in which an individual alleges that she lacks, has lost, or fears losing control over her data or personal information.[219] While this harm may arise when consumers lack or lose the ability to influence or curtail companies' use or retention of their data or information,[220] it may also occur in non-commercial contexts. In particular, in the future, an asylum-seeker may allege that, due to the persecutor's online conduct, she lacks or has lost control of her data and, significantly, she has or may suffer downstream harms resulting from the persecutor's collection, correlation, and attribution of that data.[221] Such a claim could involve a persecutor using an individual's data as both the *reason* and as a *tool* for harming the individual.[222]

There are several ways that a court could incorporate the lack or loss of control over one's data or information into a persecution determination. Under one approach, the court could categorize the lack or loss of control over one's data as an emotional or psychological harm. This approach would

---

[214] *See id.*; *see also* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753, 1778–81 (2019) [hereinafter Chesney & Citron, *Deep Fakes*] (discussing the potential emotional harm from deepfakes).

[215] *See* Imran Awan & Iren Zempi, *The Affinity Between Online and Offline Anti-Muslim Hate Crime: Dynamics and Impacts*, 27 AGGRESSION & VIOLENT BEHAVIOR 13, 21–22 (2016) (explaining that, in a victim's mind, all harms directed at a core part of the victim's identity have a greater effect than other harms); *see also* Chesney & Citron, *Deep Fakes*, *supra* note 214, at 1776–77 (providing examples of how a deepfake could be used to attribute beliefs or actions to an individual).

[216] *See* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011) (describing one category of privacy harms as the perception of unwanted observation, which includes the unwelcome mental states, such as anxiety or embarrassment, that accompany the belief that one is or will be watched or monitored).

[217] *See* Awan & Zempi, *supra* note 215, at 21–22.

[218] *See* CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 203, at 5–8 (chronicling incidents of online harm resulting in additional online and offline harm); Hum. Rts. Council, *supra* note 2, ¶1 (expressing concern that online surveillance has led to "arbitrary detention, sometimes to torture and possibly to extrajudicial killings").

[219] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 846, 853–54.

[220] *See id.* at 853.

[221] *Cf. id.* at 853.

[222] *Cf. id.* at 853 ("In the clutches of organizations, personal data can be used for a wide array of purposes for an indefinite period of time.").

align with courts' recognition that emotional and psychological harms may be persecutory,[223] and it would reflect courts' approaches outside the context of asylum law acknowledging that emotional and psychological harms may result from privacy violations.[224] Alternatively, a court could find persecution where the lack or loss of control was accompanied by or resulted in downstream harms, such as physical violence or economic deprivation.[225] This route would match courts' recognition that harms may cumulatively amount to persecution.[226] Additionally, a court may view the lack or loss of control of one's data in the context in which it occurred, finding that, in light of other events or human rights abuses in her home country, the asylum-seeker has experienced harm severe enough to rise to the level of persecution.[227] This approach would track courts' historical emphasis on contextualizing non-privacy-related harms in order to make a persecution determination.[228] Similarly, this approach reflects the emphasis on context in the privacy law sphere.[229]

Online surveillance, in particular, demonstrates how the lack or loss of control over one's data may have devastating, downstream consequences. For example, a persecutor may use data mined from an individual's online presence to associate her with marginalized, banned, or contrarian individuals, beliefs, or ideas.[230] The persecutor may then target the individual because of her actual or putative association or identification with these other individuals, beliefs, or ideas.[231] He may even harm her because of *incorrect* correlation or attribution.[232] As a result, a persecutor may then harm an individual offline, subjecting her, for example, to detention and physical violence.[233] In addition to persecuting an individual because of her data, he may also use the individual's data as a tool to harm her. For instance, he may

[223] *See, e.g.,* Ouk v. Gonzales, 464 F.3d 108, 111 (1st Cir. 2006) (recognizing emotional or psychological harm as persecutory); Mashiri v. Ashcroft, 383 F.3d 1112, 1120 (9th Cir. 2004) (similar).

[224] *See* Citron & Solove, *Privacy Harms*, *supra* note 6, at 842–45 (describing courts' recognition of emotional and psychological injuries resulting from privacy violations as cognizable harms).

[225] *See, e.g.*, Mejia v. U.S. Att'y Gen., 498 F.3d 1253, 1257–58 (11th Cir. 2007) (finding that threats and harms may cumulatively amount to persecution); Ahmed v. Keisler, 504 F.3d 1183, 1194 (9th Cir. 2007) (similar).

[226] *See Mejia*, 498 F.3d at 1257–58; *Ahmed*, 504 F.3d at 1194.

[227] *See, e.g.*, Ouda v. INS, 324 F.3d 445, 453 (6th Cir. 2003) (finding that threats and harm in the context of human rights violations amount to persecution); Korablina v. INS, 158 F.3d 1038, 1045 (9th Cir. 1998) (finding that threats and harm in the context of political and social turmoil in the home country amount to persecution).

[228] *See Ouda*, 324 F.3d at 453; *Korablina*, 158 F.3d at 1045.

[229] *See, e.g.*, Citron & Solove, *Privacy Harms*, *supra* note 6, at 818 ("Privacy harms are highly contextual, with the harm depending upon how the data is used, what data is involved, and how the data might be combined with other data.").

[230] *See, e.g.*, Anna Diamond & Larry Mitchell, *China's Surveillance State Should Scare Everyone,* THE ATLANTIC (Feb. 2, 2018), https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203 (describing the country's coordinated surveillance efforts at mining and correlating data from multiple online and offline sources about individuals' preferences and opinions).

[231] *See* Jarvis Cooper, *supra* note 5, at 765–66.

[232] *See id.*; *see also* Molly K. Land & Jay D. Aronson, *The Promise and Peril of Human Rights Technology*, *in* NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE 19 (Molly K. Land & Jay D. Aronson, eds., 2019) ("Information about us that is disclosed in one context . . . [may] be combined with other data and used in ways we could not have foreseen.") (citations omitted). *See generally* Amir Gandomi & Murtaza Haider, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, 35 INT'L J. INFO. MGMT 137 (2015) (explaining from a technical standpoint how data may be *incorrectly* correlated or attributed to individuals).

[233] *See* SHAHBAZ & FUNK, *Social Media Surveillance*, *supra* note 4 (documenting that, in 2019, social media surveillance led to 47 of the 65 countries assessed to arrest social media users for political, social, or religious speech).

use her online posts that are critical of the government to label her on social media as anti-government, putting her at risk of harm from pro-government groups.[234] As another example, a governmental persecutor may use data that he has collected from online and offline sources about an individual's ideas, as well as her online and offline associations, to assign her a profile of loyalty to the government, blacklisting her from future economic and social benefits.[235]

Using data to harm is not new; rather, "the history of the twentieth century is blood-soaked with situations in which data abetted ugly ends."[236] Thus, evidence that an individual lacks, has lost, or may lose control of her data may help to identify instances of persecution.

D. CHILLING EFFECTS

Recognizing that a persecutor's privacy-threatening conduct can chill or inhibit an individual's activities or behavior may help to identify instances of persecution.[237] For example, chilling effect harms may arise due to online surveillance and censorship.[238] As a result of online surveillance and censorship, an individual may self-censor her online presence and conduct.[239] She may also refrain from certain offline activities, such as running for political office or practicing her religion.[240] Online surveillance and censorship may also deter an individual from associating with others online or offline, including individuals with whom she shares a political opinion, religion, or other identity.[241]

---

[234] *See, e.g.*, HUM. RTS. WATCH, EVENTS OF 2020, *supra* note 2, at 543 (documenting that the military, national security agencies, and the police in the Philippines have actively used social media to threaten and label individuals as communists, resulting in multiple deaths and putting those individuals at a heightened risk for other offline harms).

[235] *See, e.g.*, Diamond & Mitchell, *supra* note 230 (describing how the Chinese government will assign profiles of loyalty based on data that has been collected via online and offline surveillance*)*; *see also* Xiao Qiang, *President Xi's Surveillance State*, 30 J. DEMOCRACY 53, 59–60 (2019) (describing China's "social credit system" gathered from online and offline sources).

[236] VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 151–52 (2013) (providing the example of the Nazis' use of the Netherlands' comprehensive civil records to identify Jewish individuals).

[237] *Cf.* Citron & Solove, *Privacy Harms*, *supra* note 6, at 854–55; *see also* Penney, *Online Surveillance and Wikipedia Use*, *supra* note 89, at 125.

[238] *See* Penney, *Online Surveillance and Wikipedia Use*, *supra* note 89, at 160–64 (documenting empirically that, following widespread publicity about the U.S. government's mass surveillance efforts, online traffic to privacy-sensitive Wikipedia articles decreased).

[239] *See, e.g.*, Marilyn Clark & Anna Grech, COUNCIL OF EUROPE, *Journalists under pressure - Unwarranted interference, fear and self-censorship in Europe* 13 (2017), https://rm.coe.int/CoERM PublicCommonSearchServices/DisplayDCTMContent?documentId=090000168070ad5d (documenting self-censorship by journalists subjected to targeted surveillance); *see also* Avetisyan v. Gonzales, 177 F. App'x 760, 762 (9th Cir. 2006) (noting, in a case finding that a journalist had been persecuted, that journalists in the asylum-seeker's home country frequently engage in self-censorship and that there is retaliation against those who do not). *Cf.* Matheus v. U.S. Att'y Gen., 757 F. App'x 803, 807 (11th Cir. 2018) (addressing a case in which an applicant seeking CAT protection was threatened with physical violence after refusing to censor anti-government comments posted on his blog).

[240] *Cf.* Zhang v. Ashcroft, 388 F.3d 713, 718 (9th Cir. 2004) (noting that the asylum-seeker's parents were "subjected to ongoing house searches and constant surveillance, making them fearful and unable to practice Falun Gong").

[241] *See* Tamar Megiddo, *Online Activism, Digital Domination, and the Rule of Trolls: Mapping and Theorizing Technological Oppression by Governments*, 58 COLUM. J. TRANSNAT'L L. 394, 400–01 (2020) (explaining that dissidents and individuals who are active online purposefully seek others' online engagement).

While there are no asylum cases specifically categorizing the harms resulting from online surveillance and censorship as chilling effect harms, future asylum claims will include allegations that a persecutor's online conduct chilled or inhibited an individual's online activities, behavior, or presence.[242] Indeed, the press regularly reports that governments[243] and non-state actors, including social media platforms[244] and telecommunication companies,[245] engage in online surveillance and censorship.

How, then, can chilling effects be addressed in the context of asylum claims? In a nutshell, evidence that an individual's liberties or activities have been chilled may be evidence of persecution. Significantly, a persecutor's chilling conduct may discourage an individual from communicating with others about her race, religion, nationality, social group, or political opinion.[246] Indeed, one of the *main* reasons that a persecutor may engage in persecution—either offline or online—is to force the targeted individual to suppress or even abandon her identification with her race, religion, nationality, social group, or political opinion.[247] The persecutor's goal is to drown out dissenting voices and prevent those voices from reaching others.[248] As Judge Richard Posner observed, "[o]ne aim of persecuting a religion is to drive its adherents underground in the hope that their beliefs will not infect the remaining population."[249] In short, the persecutor's conduct can create a *persecutory environment*[250]—either offline or online—that may have a profound chilling effect on an individual's expression of and

---

[242] *See* SHAHBAZ & FUNK, *Social Media Surveillance*, *supra* note 4.

[243] *See, e.g.*, Pei Li, *China Punishes Microblog Platform Weibo for Interfering with Communication*, REUTERS (June 10, 2020), https://reut.rs/2UvETbT (reporting that the Chinese government censors the microblog platform, Weibo).

[244] *See, e.g.*, AFP, *Israeli Hosting Firm Wix Removes Hong Kong Democracy Website After Police Order,* TIMES OF ISRAEL (June 5, 2021), https://www.timesofisrael.com/israeli-hosting-firm-wix-removes-hong-kong-democracy-website-after-police-order (reporting that an Israeli web hosting firm removed a pro-democracy website at the request of the Chinese police); Jeb Su, *Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine*, FORBES (July 19, 2019), https://www.forbes.com/sites/jeanbaptiste/2019/07/19/confirmed-googleterminated-project-dragonfly-its-censored-chinese-search-engine (discussing Google's prior project facilitating the Chinese government's online censorship).

[245] *See, e.g.*, Joe Parkinson, Nicholas Bariyo & Josh Chin, *Huawei Technicians Helped African Governments Spy on Political Opponents*, WALL ST. J. (Aug. 15, 2019), https://www.wsj.com/articles/huaweitechnicians-helped-african-governments-spy-on-political-opponents-11565793017?mod=e2tw [https://perma.cc/NW5W-MRCX] (reporting that local employees of the telecommunications company Huawei helped the Ugandan and Zambian governments surveil their political opponents' WhatsApp and Facebook accounts, leading to the opponents' arrests).

[246] *See, e.g.*, Zhang v. Ashcroft, 388 F.3d 713, 718 (9th Cir. 2004) (noting that, due to surveillance, the asylum-seeker's mother was afraid to practice Falun Gong in the park). *Cf.* HUM. RTS. WATCH, EVENTS OF 2020, *supra* note 2, at 169 (documenting that government authorities shut down the only Mongolian-language social media site in China). *See generally* Margaret E. Roberts, *Resilience to Online Censorship*, 23 ANNUAL REV. OF POL. SCI. 403 (2020) [hereinafter Roberts, *Resilience to Online Censorship*] (explaining the mechanisms by which online censorship technologies discourage users from accessing or spreading information).

[247] *See* Muhur v. Ashcroft, 355 F.3d 958, 961 (7th Cir. 2004) (Posner, J.).

[248] *See* Tiberiu Dragu & Yonatan Lupu, *Digital Authoritarianism and the Future of Human Rights*, INT'L ORG. 6 (2021) (documenting that governmental persecutors engage in online measures to prevent or reduce dissent).

[249] *Muhur*, 355 F.3d at 960.

[250] *See* MATTHEW SCOTT, CLIMATE CHANGE, DISASTERS, AND THE REFUGEE CONVENTION 107–10 (James Hathaway ed., Cambridge Univ. Press 2020) (explaining, in the context of international refugee law, that an individual is "being persecuted" if she inhabits a persecutory social environment—a condition of existence in which her government may fail to protect her from a denial of a human right under international law).

ability to share her beliefs, opinions, or identity, especially as they relate to her race, religion, nationality, social group, or political opinion.

Crucially, U.S. law does not condition asylum eligibility on an individual taking steps to avoid persecution.[251] This emphasis on not placing a burden on the victim of persecution to avoid persecution is highly significant in general and specifically with respect to privacy harms. For example, an asylum-seeker is not required to demonstrate that she devised or could have devised a work-around to the persecutor's online conduct, such as communicating via an encrypted or offline channel to avoid surveillance or using a virtual private network to access censored or blocked websites or content.[252] An individual is also not required to show that she hid or could have hid her beliefs, opinions, or identity to avoid persecution.[253] For example, a privacy harm is not necessarily mitigated if an individual could have telegraphed her religious beliefs or political opinion through coded or indirect communication online, such as using symbols, words, or hashtags that are not readily decipherable by a persecutor.[254] Thus, there is no burden on an asylum-seeker to show that she could or should have avoided the privacy harm.

U.S. asylum law even considers any requirement that an individual conceal or abandon her identification with a protected identity as a form of persecution in its own right.[255] By extension, with a few exceptions,[256] an individual must be permitted to identify or associate with or communicate about her race, religion, nationality, social group, or political opinion "in a manner, through a medium, and with an audience of her choosing."[257] In other words, any attempt to prevent how and with whom an individual chooses to practice her religion or identify with another protected ground may be inherently persecutory.[258] For example, online surveillance that

[251] *See, e.g.*, Antipova v. U.S. Att'y Gen., 392 F.3d 1259, 1265 (11th Cir. 2004) (explaining that a persecution determination "cannot be discharged by asking whether the applicant could have somehow avoided the past persecution").

[252] *See, e.g.*, William R. Hobbs & Margaret E. Roberts, *How Sudden Censorship Can Increase Access to Information*, 3 AMER. POL. SCI. REV. 626–33 (2018) (describing social media users' work-around strategies to censorship by the Chinese government).

[253] *See Antipova*, 392 F.3d at 1264–65 (noting that asylum-seekers who have been persecuted in the past on account of a protected ground are not required "to avoid signaling to others that they are indeed members of a particular race, or adherents of a certain religion, etc."); Velasquez-Banegas v. Lynch, 846 F.3d 258, 262 (7th Cir. 2017) (noting that asylum-seekers fearing future persecution are not required "to hide characteristics like religion or sexual orientation, and medical conditions, such as being HIV positive") (citation omitted).

[254] *See, e.g.*, Muhur v. Ashcroft, 355 F.3d 958, 960 (7th Cir. 2004) (holding that it is a clear error of law to assume that an individual is not entitled to asylum if she could "escape notice of the persecutors by concealing one's religion").

[255] *See* Guo v. Sessions, 897 F.3d 1208, 1216 (9th Cir. 2018) (finding that governmental actions that force an asylum-seeker to abandon his religious worship amount to past persecution); Kazemzadeh v. U.S. Att'y Gen., 577 F.3d 1341, 1357 (11th Cir. 2009) (Marcus, J., concurring) (noting that "any requirement that Kazemzadeh abandon his faith or practice in secret in order to conceal his conversion amounts to religious persecution under our asylum laws"); *see also* Shi v. U.S. Att'y Gen., 707 F.3d 1231, 1236 (11th Cir. 2013) (citing *Kazemzadeh*, 577 F.3d at 1358–60).

[256] *See* 8 C.F.R. §§ 208.4, 208.13, 208.14, 1208.4, 1208.13, 1208.14 (listing bars to asylum, including the prohibition against granting asylum to serious criminals, persecutors, and terrorists).

[257] Jarvis Cooper, *supra* note 5, at 768.

[258] *Cf.* Woldemichael v. Ashcroft, 448 F.3d 1000, 1003 (8th Cir. 2006) ("Absent physical harm, subjecting members of an unpopular faith to hositility, harassment, discrimination, and even economic deprivation is not persecution unless those persons are prevented from practicing their religion or deprived of their freedom.") (citing Nagoulko v. INS, 333 F.3d 1012, 1016 (9th Cir. 2003)).

inhibits an individual from blogging about her religion may amount to persecution, even if there had been or could be alternate routes for religious self-expression.[259] Thus, recognizing when and how a persecutor's conduct may chill an individual's online or offline activities, behavior, or presence may help to identify persecution.

E. MANIPULATION

Identifying instances of manipulation will help courts and adjudicators to recognize when persecution has occurred or may occur. In Citron and Solove's typology, manipulation is an autonomy harm involving the "undue influence over people's behavior or decision-making."[260] As Ido Kilovaty notes, manipulation "effectively deprives individuals of their agency by distorting and perverting the way in which individuals typically make decisions."[261] The classic example is voter manipulation.[262]

While there are no asylum cases specifically addressing manipulation as evidence of persecution, such claims are likely to arise in the future due to online or digital manipulation. Indeed, research has documented that governments are actively engaged in organized online manipulation campaigns to shape public opinion, spread disinformation, attack and discredit political opponents, and drown out dissenting opinions.[263] Online governmental manipulation may even include directing or influencing online trolls and non-state actors to carry out or propagate the online manipulation.[264]

Given the significance that online manipulation may have in future asylum claims,[265] it is important to expand on what it entails. To begin with, online manipulation is an unprecedented form of harm.[266] As Ryan Calo explains, online manipulation uniquely combines "*personalization* with the intense *systemization* made possible by mediated consumption."[267] In other words, individuals can now be systematically manipulated through the technologies that they use in daily life.[268]

Persecutors may engage in online manipulation through a variety of ways. For example, persecutors may target specific audiences with tailored messaging based on information gleaned from those individuals' social

---

[259] *See* Jarvis Cooper, *supra* note 5, at 768.

[260] Citron & Solove, *Privacy Harms*, *supra* note 6, at 845–46.

[261] Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 469 (2019) (citations omitted).

[262] *See, e.g.*, Susser et al., *supra* note 95, at 9–12.

[263] *See* SHAHBAZ & FUNK, *Social Media Surveillance*, *supra* note 4; Samantha Bradshaw & Philip N. Howard, THE GLOBAL DISINFORMATION ORDER: 2019 GLOBAL INVENTORY OF ORGANISED SOCIAL MEDIA MANIPULATION 2, 15 (2019), https://perma.cc/TRS8-5KJ5 (finding, as of 2019, evidence of organized social media manipulation campaigns in 70 countries).

[264] *See* Megiddo, *supra* note 241, at 395–425, 439–40 (examining governments' harnessing of non-state actors to fulfill their agendas of online harm); *see also* Claire Wardle, *A New World Disorder*, SCIENTIFIC AM., Sept. 2019, at 84 (explaining how and why bad actors weaponize social media users as unwitting agents of disinformation).

[265] *See* SHAHBAZ & FUNK, *Social Media Surveillance*, *supra* note 4; Bradshaw & Howard, *supra* note 263, at 2.

[266] *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1002 n.33, 1021 (2014) (discussing this unprecedented phenomenon with respect to digital market manipulation).

[267] *Id.* at 1021 (emphasis in the original).

[268] *See id.*; *see also* Ronald Deibert, *Three Painful Truths about Social Media*, 30 J. DEMOCRACY 25, 28–31 (2019) (describing how social media platforms manipulate users).

media profiles.[269] At the same time, both government and non-state actors may disseminate disinformation to distract, confuse, or overwhelm their target audience, as well as control or highjack the online and offline discourse.[270] Persecutors may also flood online communication channels with their messaging to drown out opposing or dissident voices.[271] Persecutors' content may even include non-controversial, pro-regime messaging in an attempt to shift the conversation away from controversial issues.[272] Recognizing that awareness of visible censorship may result in a backlash, persecutors may engage in partial or subtle forms of censorship, such as controlling search engine results or selectively removing social media posts.[273] Persecutors may even rely on the technical complexity of the internet to manipulate their targets.[274] For example, they may rely on users' inability to distinguish between a bona fide power outage or blackout and a controlled, purposeful restriction in online access.[275] Thus, online manipulation can be subtle, involve tailored information, create echo chambers, and ultimately influence people's behavior such that they no longer participate in meaningful political, cultural, religious, or social discourse.[276] Individuals may even be lulled into no longer feeling uncomfortable with their government's offline and online persecution.[277] And, critically, the online manipulation can take place across different technologies, ranging from social media to digital assistants.[278] In this way, due to its pervasiveness and efficacy in influencing thoughts and behavior, *online* manipulation may be legally distinguishable from *offline* manipulation.[279] In other words, persecutors' online manipulation of the

[269] *See* Megiddo, *supra* note 241, at 419 (explaining the practice of creating detailed profiles on social media users which are then used for "micro-targeting," including to further pernicious ends such as voter suppression).

[270] *See* Ekaterina Zhuravskaya, Maria Petrova & Ruben Enikolopov, *Political Effects of the Internet and Social Media*, 12 ANNUAL REV. OF ECON. 431 (2020).

[271] *See* Megiddo, *supra* note 241, at 416 (explaining that "[d]isinformation is often coupled with an attempt to 'drown-out' oppositional messages by circulating counter-messages on a wide scale in an attempt to dominate the conversations online").

[272] *See, e.g.*, Gary King, Jennifer Pan & Margaret E. Roberts, *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*, 3 AM. POL. SCI. REV. 483, 485 (2017) (documenting that, rather than defending the government or addressing controversial issues, the Chinese government posts content on social media that focuses on cheerleading for China to distract the public and direct its attention away from discussions or events with collective action potential).

[273] *See* Roberts, *Resilience to Online Censorship*, *supra* note 246, at 408–10.

[274] *See id.* at 409.

[275] *See id.*

[276] *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1917 (2013) (explaining that the networked processes of surveillance and modulation are more than systems for manufacturing consent but, rather, are subtle processes of continual feedback in which stimuli are tailored to play to existing inclinations, nudging individuals along inclinations and confining them to "filter bubbles" that conform the information environment to their ideologies).

[277] *See id.* at 1918 ("Liberal democratic citizenship requires a certain amount of discomfort—enough to motivate citizens to pursue improvements in the realization of political and social ideals. The modulated citizenry lacks the wherewithal and perhaps even the desire to practice this sort of citizenship.").

[278] *See, e.g.*, Stucke & Ezrachi, *supra* note 27, at 1270–78 (explaining how digital assistants can be used as tools to manipulate individuals' beliefs and amplify some ideas over others).

[279] *Contra* Qing Chen v. U.S. Att'y Gen., 428 F. App'x 212, 215 (3d Cir. 2011) (finding that, despite evidence indicating that there has been an increase in online censorship and "manipulation of the press and internet," the Chinese government's online efforts reflect an extension of its historical offline persecution).

internet is not necessarily a continuation of their offline censorship, surveillance, or propaganda efforts.[280]

Like other forms of online conduct and types of privacy harms discussed in this Article, online manipulation may be evidence of persecution. Why would a persecutor engage in online manipulation? The short answer is to stay in power by suffocating dissent.[281] To do so, a persecutor may try to trick an individual into restricting, suppressing, abandoning, or even renouncing her beliefs, opinions, or identity.[282] A persecutor's intent is to force an individual into the offline or cyber underground, keeping her beliefs, opinions, and identity out of circulation and from influencing others.[283] In other words, his goal is to manipulate the individual away from being an online voice of dissent.[284] An individual may even, then, be manipulated into making different choices about her offline conduct: she may be discouraged, for example, from voting, engaging in political protests, or attending religious services.

Even being "beneficially" or "benevolently" influenced into restricting, suppressing, abandoning, or renouncing one's beliefs, opinions, or identity may count as persecutory manipulation.[285] Thus, a practitioner of a minority religion who is influenced to forsake her beliefs may subsequently find that her apostasy elevates her in society, but, nonetheless, she may still have been manipulated. Under U.S. asylum law, the relevance of such supposedly beneficial or benevolent manipulation will turn on the asylum-seeker's perception of the manipulation: while she may have benefited from the manipulation, she may still perceive the manipulation as past persecutory harm,[286] as well as evidence that she will be persecuted in the future.[287] Moreover, the persecutor's *intent* to engage in "benevolent" or "beneficial" manipulation is irrelevant to a persecution determination under U.S. asylum law.[288] As Judge John T. Noonan Jr. explained, "[w]hether an act is or is not

---

[280] *Contra id.*

[281] *See generally* Sergei Guriev & Daniel Treisman, *A Theory of Informational Autocracy*, 186 J. OF PUB. ECON. (2020) (proposing the theory of informational autocracy to describe how "incompetent dictators manipulate information to stay in power").

[282] *See* Shoshana Zuboff, *"We Make Them Dance": Surveillance Capitalism, the Rise of Instrumentarian Power, and the Threat to Human Rights*, in HUMAN RIGHTS IN THE AGE OF PLATFORMS 22–23 (Rikke Frank Jorgensen, ed. 2019) (explaining how individuals are subtly conditioned online to make different choices); *see also* Muhur v. Ashcroft, 355 F.3d 958, 961 (7th Cir. 2004) (Posner, J.) (explaining that persecutors seek to drive individuals and their beliefs into the underground so that they do not influence others).

[283] *See Muhur*, 355 F.3d at 960.

[284] *See* Dragu & Lupu, *supra* note 248, at 6.

[285] *See* Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MARKETING BEHAV. 213, 225 (2015) ("Some acts of manipulation count as such even if they leave the chooser better off. (You might be manipulated to purchase a car that you end up much enjoying.) We might say that such acts are justified—but they are manipulative all the same.").

[286] *Cf.* Ordonez-Quino v. Holder, 760 F.3d 80, 90–92 (1st Cir. 2014) (finding that a child's point of view must be considered in evaluating whether the past harm amounts to persecution); Rusak v. Holder, 734 F.3d 894, 897 (9th Cir. 2013); Jorge-Tzoc v. Gonzales, 435 F.3d 146, 150–51 (2d Cir. 2006); Abay v. Ashcroft, 368 F.3d 634, 640 (6th Cir. 2004); Liu v. Ashcroft, 380 F.3d 307, 313–14 (7th Cir. 2004); USCIS PAST PERSECUTION GUIDANCE, *supra* note 118, § 3.2.5 (recommending consideration of an elderly individual's point of view when evaluating whether harm amounts to persecution).

[287] *See, e.g.*, Parada v. Sessions, 902 F.3d 901, 909 (9th Cir. 2018) (finding that an individual may establish her subjective fear of future persecution through her credible testimony that she genuinely fears harm); Ahmed v. Keisler, 504 F.3d 1183, 1191 (9th Cir. 2007) (similar).

[288] *See* Montecino v. INS, 915 F.2d 518, 520 (9th Cir. 1990).

persecution cannot depend on whether it is rational or strategic from the point of view of the persecutors."[289]

Persecutors may also seek to manipulate others about a race, religion, nationality, social group, or political opinion. For example, a governmental persecutor may manipulate social media users into not voting for a political opponent.[290] The persecutor's online manipulation may even influence how others treat another individual or group because of their protected identity. For example, by framing the online discourse around a group, a persecutor may ostracize the group from society, increasing the likelihood that the group will be targeted with physical violence offline.[291] In other words, while online manipulation may lead to privacy harms affecting individual asylum-seekers, online manipulation may also influence group behavior and incite persecution.

As the privacy literature has discussed whether manipulation is provable,[292] it is important to expand on how U.S. asylum law could address this issue. To begin with, it is well-established that immigration proceedings do not adhere to strict rules of evidence.[293] For example, an asylum-seeker's proffered hearsay evidence is admissible, although an immigration judge or the Board may accord it less weight than non-hearsay evidence.[294] This flexibility in admissibility must similarly be extended to the asylum-seeker's evidence involving the online realm, including evidence of online manipulation.

Next, recognizing that an individual may have difficulty obtaining evidence before and after fleeing from persecution,[295] U.S. asylum law is generally flexible in what types of evidence may establish asylum eligibility.[296] To be eligible for asylum, an individual must provide some indication of what the persecutor did or may do to her or others that causes

---

[289] *Id.* (Noonan, J.).

[290] *See* Susser et al., *supra* note 95, at 9–12.

[291] *See, e.g.*, HUM. RTS. WATCH, EVENTS OF 2020, *supra* note 2, at 543 (documenting that the military, national security agencies, and the police in the Philippines have actively used social media to threaten and label individuals as communists, putting those individuals at a heightened risk for offline harm and resulting in many of their deaths).

[292] *See, e.g.*, Shaun Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 997–98 (2020) (discussing the difficulty in proving that a consumer was manipulated).

[293] *See, e.g.*, Dallo v. INS, 765 F.2d 581, 586 (6th Cir. 1985); Matter of Wadud, 19 I&N Dec. 182, 188 (BIA 1984); Baliza v. INS, 709 F.2d 1231, 1233 (9th Cir. 1983).

[294] *See, e.g.*, Gu v. Gonzales, 454 F.3d 1014, 1021 (9th Cir. 2006) (admitting an asylum-seeker's credible testimony consisting of hearsay evidence from an anonymous friend); Dia v. Ashcroft, 353 F.3d 228, 254 (3d Cir. 2003) (en banc) (providing that an asylum-seeker's proffered hearsay evidence is admissible but may be accorded less evidentiary weight). In removal and deportation proceedings, courts have based admissibility of the government's proffered evidence, including hearsay, on whether the evidence is probative and its admission is fundamentally fair to the asylum-seeker. *See, e.g.*, Espinoza v. INS, 45 F. 3d 308, 310 (9th Cir. 1995) (citing Trias-Hernandez v. INS, 528 F.2d 366, 369 (9th Cir. 1975)); Tashnizi v. INS, 585 F.2d 781, 783–84 (5th Cir. 1978); *see also* 8 C.F.R. §§ 1240.7(a), 1240.46(c) (2022) (addressing evidence in removal proceedings).

[295] *See, e.g.*, Solomon v. Gonzales, 454 F.3d 1160, 1164–65 (10th Cir. 2006); Wiransane v. Ashcroft, 366 F.3d 889, 897 (10th Cir. 2004); Senathirajah v. INS, 157 F.3d 210, 215–16 (3d Cir. 1998); *see also* U.S. DEPT. OF JUSTICE, IMMIGR. NATZ. SERV., *Aliens and Nationality; Asylum and Withholding of Deportation Procedures*, 53 Fed. Reg. 11,300, 11,302 (Apr. 6, 1988).

[296] *See, e.g.*, 8 U.S.C. § 1158(b)(1)(B)(ii); *see also* Sangha v. INS, 103 F.3d 1482, 1487 (9th Cir. 1997) (noting, in a case pre-dating the REAL ID Act of 2005, Pub. L. 109–13, 119 Stat. 302, that "[b]ecause asylum cases are inherently difficult to prove, an applicant may establish his case through his own testimony alone") (citation omitted).

her to seek asylum.[297] However, an asylum-seeker can satisfy her evidentiary burden through her credible testimony alone. Even when a court or adjudicator requests evidence corroborating an asylum-seeker's testimony, an asylum-seeker is not required to provide such evidence if she cannot reasonably obtain it.[298] An individual may also establish her asylum eligibility through circumstantial evidence.[299]

Thus, under U.S. asylum law, an asylum-seeker is not and should not be categorically required to provide direct, expert, or corroborating evidence that online manipulation occurred. Moreover, there may be times when direct, expert, or corroborating evidence of a persecutor's online manipulation or other conduct does not exist. There may also be times when, even if such evidence exits, it is not reasonably obtainable.[300] While direct, expert, or corroborating evidence may be relevant and helpful, the asylum-seeker's credible testimony, circumstantial evidence, or a combination of the two, may be sufficient to establish that online manipulation occurred. For example, an asylum-seeker's *belief* that she was manipulated on Facebook, along with an explanation as to why she arrived at that belief, such as circumstantial evidence that the persecutor *may* be involved in an online disinformation campaign,[301] could be enough to establish that online manipulation occurred.

As Citron and Solove have noted, people respond differently to manipulation, and some individuals might not even realize that they have been manipulated.[302] Along these lines, an asylum-seeker can certainly present evidence explaining why, due to her vulnerabilities or experiences, she was manipulated, including information on why she was more susceptible to manipulation than another individual.[303] However, she should not be categorically denied asylum just because she was manipulated by the persecutor's online conduct when others were not or might not be.

Finally, with respect to the alleged manipulator's intent,[304] it is important to point out that U.S. asylum law does not require an asylum-seeker to prove that a persecutor intended to punish or inflict harm.[305] For instance, an

---

[297] *See* 8 U.S.C. § 1158(b)(1)(B)(i); 8 C.F.R. §§ 208.13(a), (b), 1208.13(a), (b).

[298] *See* 8 U.S.C. § 1158(b)(1)(B)(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a).

[299] *See, e.g.*, Madrigal v. Holder, 716 F.3d 499, 505 (9th Cir. 2013) ("Although it is [the asylum-seeker's] burden to establish his eligibility for asylum, he may satisfy this burden with circumstantial evidence."); *see also* Karouni v. Gonzales, 399 F.3d 1163, 1174 (9th Cir. 2005) (recognizing circumstantial evidence of a persecutor's identity); INS v. Elias-Zacarias, 502 U.S. 478, 483 (1992) (recognizing circumstantial evidence of a persecutory nexus).

[300] *See* 8 U.S.C. § 1158(b)(1)(B)(ii); 8 C.F.R. §§ 208.13(a), 1208.13(a). *Contra* Pocasangre Garcia v. Garland, No. 20-70307 *3 (9th Cir. June 7, 2021) (finding that an asylum-seeker failed to explain why threatening Facebook messages from her ex-boyfriend were not available and assuming that it is reasonable for an asylum-seeker to contact Facebook for help in recovering such messages).

[301] *See, e.g.*, Carme Colomina, Héctor Sánchez Margalef & Richard Youngs, Directorate General for External Policies of the Union, European Parliament, *The impact of disinformation on democratic processes and human rights in the world*, PE 653.635, ¶ 2.2 (Apr. 2021).

[302] Citron & Solove, *Privacy Harms*, *supra* note 6, at 848.

[303] *See, e.g.*, Ordonez-Quino v. Holder, 760 F.3d 80, 90–92 (1st Cir. 2014) (recognizing the significance of a child's vulnerabilities in assessing persecution); USCIS PAST PERSECUTION GUIDANCE, *supra* note 118, § 3.2.5 (recognizing the significance of an elderly individual's vulnerabilities in assessing persecution).

[304] *See, e.g.*, Spencer, *supra* note 292, at 989 (explaining that several definitions of manipulation require intent by the alleged manipulator); *see also* Citron & Solove, *Privacy Harms*, *supra* note 6, at 847.

[305] *See, e.g.,* Pitcherskaia v. INS, 118 F.3d 641, 646 (9th Cir. 1997) ("Neither the Supreme Court nor this court has construed the Act as imposing a requirement that the alien prove that her persecutor was

asylum-seeker does not need to prove that the persecutor manipulated her to cause her emotional trauma. Rather, the asylum-seeker only needs to prove that the persecutor was motivated to engage in the online conduct because of the asylum-seeker's actual or imputed race, religion, nationality, particular social group, or political opinion.[306]

Thus, as this Part has shown, there are multiple privacy harms that may be implicated in asylum claims. Some harms, such as economic and psychological privacy harms, can be analogized to their non-privacy counterparts that have already been recognized as persecutory. Other harms, such as lack of control, chilling effect, or manipulation privacy harms, can similarly be evidence of persecution.

V. CONCLUSION

This Article has suggested several frameworks for addressing asylum claims alleging privacy harms, including the novel idea that an online privacy harm may be tantamount to online persecution. As the discourse around privacy harms in asylum claims moves forward, we, as Americans, must remain conscious of our position of power in which we determine who receives asylum and why. We must also remember that our perception of whether a privacy harm amounts to persecution may be influenced—that is, either limited or enhanced—by our prior experiences[307] and cultural perspectives.[308] In other words, we must listen carefully to and respect an individual's experience of past privacy harms and her fear of future persecution. After all, "[p]rivacy harm is largely in the eyes of the juridical beholder."[309] Finally, we must remember that U.S. asylum law is not and should not be static. U.S. asylum law must continue to evolve, recognizing the new ways that individuals, governments, and others communicate—and do harm—via digital technologies and in the online realm.[310]

motivated by a desire to punish or inflict harm."); *see also* Mohammed v. Gonzales, 400 F.3d 785, 796 n.15 (9th Cir. 2005) ("Persecution simply requires that the perpetrator cause the victim suffering or harm and does not require that the perpetrator believe that the victim has committed a crime or some wrong.") (quotation marks omitted) (quoting *Pitcherskaia*, 118 F.3d at 647–48).

[306] *See* INS v. Elias-Zacarias, 502 U.S. 478, 481–82 (1992) (requiring a nexus between a persecutor's reasons for harming an individual and the individual's identification or association with one of the five protected grounds of asylum).

[307] *See* Elizabeth Riedford, Who Do You Think I Am? A Qualitative Study on How Professional and Cultural Experience of Adjudicators Affects Perception of Asylum Seekers 5, 97–115 (2020) (Ph.D. dissertation, Northeastern University), https://repository.library.northeastern.edu/files/neu:m046pd55c/fulltext.pdf (documenting that, among other factors, asylum adjudications are influenced by asylum officers' prior professional experiences). *See generally* Fatma E. Marouf, *Implicit Bias and Immigration Courts*, 45 NEW ENG. L. REV. 417 (2011).

[308] *See* Payal Arora, *Decolonizing Privacy Studies*, 20(4) TELEVISION & NEW MEDIA 366–78 (2019) (arguing that privacy is culturally defined and calling for alternative meanings of privacy that reflect those cultural differences).

[309] Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 46 (2019).

[310] *See* Jarvis Cooper, *supra* note 5, at 778–79, 781–82.