A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law

Madison Lo*

Tactics of domestic violence are nothing new. However, as with various other aspects of modern life, technology threatens disruption.

The increasing prevalence of Internet of Things (IoT) devices has given abusers a powerful new tool to expand and magnify the traditional harms of domestic violence, threatening the progress advocates have made in the past thirty years and creating novel dangers for survivors. An IoT device is a "smart," stand-alone, internet-connected device that can be monitored or controlled from a remote location. They are cheap and increasingly common—the number of IoT-enabled devices in the world is already in the billions and expected to grow quickly. IoT devices allow abusers to overcome geographic and spatial boundaries that would have otherwise prevented them from monitoring, controlling, harassing, and threatening survivors.

Various advocates are finding ways to protect survivors, and the broader public, from these new dangers. In the domestic violence sphere, domestic violence service providers are creating resources for survivors that explain IoT-facilitated abuse and how to better secure their smart devices. In the technology sphere, consumers, businesses, digital experts, and the media are broadcasting the security risks of IoT devices. Unfortunately, significantly fewer outlets describe the legal remedies available for IoT-facilitated abuse.

DOI: https://doi.org/10.15779/Z38XW47X1J.

* J.D. Candidate, 2021, University of California, Berkeley, School of Law; B.A., 2018, The University of Chicago. I am grateful to Professor Nancy K. D. Lemon for her guidance on earlier drafts, and to all my classmates in Professor Lemon's Domestic Violence Seminar for inspiring me with their empathy and critical viewpoints. I also want to thank the editors of the *California Law Review* for believing in this piece and providing invaluable feedback. This Note would not be possible without their contributions.

This Note aims to bridge that gap. It demonstrates that IoT-facilitated abuse is a form of technology-facilitated domestic violence and explores how society can use current laws to address IoT-facilitated abuse. However, it also questions whether the existing remedies are sufficient and offers recommendations for legal and non-legal changes that will better protect survivors of IoT-facilitated abuse and hold perpetrators accountable.

INTRODUCTION

U.S. society is becoming increasingly digital. A 2019 study found that 86 percent of Americans use the internet daily.[1] Americans increasingly conduct

1. WE ARE SOC., DIGITAL IN 2019: THE UNITED STATES OF AMERICA 23 (2019), https://wearesocial.com/us/digital-2019-us [https://perma.cc/ZX4S-S65P]. Preliminary research on

important transactions electronically, from making banking and travel arrangements, to accessing legal and medical records.[2] The COVID-19 pandemic has forced even more social and commercial activities to migrate online.[3] With the unique advantages of technology also come new dangers when these technologies are misused. According to a 2014 survey by the National Network to End Domestic Violence's (NNEDV) Safety Net Project, 97 percent of domestic violence service providers reported that the survivors they work with experience harassment, monitoring, and threats from their abusers through technology.[4]

Much research on technology-facilitated domestic violence concentrates on "conventional" cyber risks such as abuse via social media and phones.[5] But there is a newer area of technology that deserves greater attention: the "Internet of Things," or the "IoT," a term describing the network of stand-alone internet-connected devices that individuals can monitor or control from a remote location.[6] While there is hardly any legal research focusing on IoT-facilitated domestic violence, the existing research on the intersection of domestic violence and technology can inform responses to IoT-facilitated abuse. This Note thus aims to explain why IoT-facilitated abuse is a form of domestic violence and specifically of technology-facilitated abuse ("tech abuse"), while highlighting its unique characteristics and implications.

Part I provides background on domestic violence and technology-facilitated abuse. Part II provides a comprehensive definition of the IoT, explains how IoT-facilitated abuse is a form of domestic violence, and explores various ways in

---

Internet usage during the COVID-19 pandemic reveals that internet traffic has surged up to 70 percent. Mark Beech, *COVID-19 Pushes Up Internet Use 70% and Streaming More Than 12%, First Figures Reveal*, FORBES (Mar. 25, 2020, 3:49 PM), https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal [https://perma.cc/6VXK-39UW].

2. Andrew King-Ries, *Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future?*, 20 TEX. J. WOMEN & L. 131, 139 (2011).

3. Emily A. Vogels, *From Virtual Parties to Ordering Food, How Americans Are Using the Internet During COVID-19*, PEW RSCH. CTR. (Apr. 30, 2020), https://www.pewresearch.org/fact-tank/2020/04/30/from-virtual-parties-to-ordering-food-how-americans-are-using-the-internet-during-covid-19 [https://perma.cc/39Y9-FWEY] (describing how social activities, fitness, ordering meals, and education have moved to the internet).

4. NAT'L NETWORK TO END DOMESTIC VIOLENCE, A GLIMPSE FROM THE FIELD: HOW ABUSERS ARE MISUSING TECHNOLOGY 1 (2014), https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455a0/1424216502058/NNEDV_Glimpse+From+the+Field+-+2014.pdf [https://perma.cc/X7KH-ELDC].

5. Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis & Leonie Tanczer, '*Internet of Things': How Abuse Is Getting Smarter*, 64 SAFE – DOMESTIC ABUSE Q., 2019, at 22, 24.

6. Andrew Meola, *What Is the Internet of Things? What IoT Means and How It Works*, BUS. INSIDER (May 10, 2018, 1:06 PM), https://www.businessinsider.com/internet-of-things-definition [https://perma.cc/2ZFT-WANA].

which IoT-facilitated abuse presents challenges for survivors[7] and advocates. Finally, Part III explores remedies and surveys various ways in which society may utilize current civil and criminal laws in cases of IoT-facilitated abuse. It ultimately argues that such remedies are insufficient because courts may not interpret current laws in a way that protects survivors of IoT-facilitated abuse, and because the process of seeking legal remedies (particularly in the criminal justice system) can re-traumatize or even endanger survivors and their communities. Whenever possible, Part III also provides suggestions for legal and non-legal changes that will better keep survivors of IoT-facilitated abuse safe and hold their abusers accountable.

I.
BACKGROUND

This Section describes the characteristics of domestic violence and tech abuse in order to situate IoT-facilitated abuse within both of those broader categories. The characteristics of domestic violence apply to all forms of abuse, including IoT-facilitated abuse. This relationship is critical in evaluating and crafting remedies because the most effective remedies will address IoT-facilitated abuse as part of a system of harm and not as isolated incidents of technology misuse. Although technology has altered and expanded the instruments of domestic violence, perpetrators of IoT-facilitated abuse still use tactics of control, manipulation, harassment, surveillance, and revenge. This Section also describes a few common methods of tech abuse to demonstrate its scope and to provide a point of comparison for Part II's discussion of the unique implications of IoT-facilitated abuse.

A. Domestic Violence Generally

Domestic violence—also called intimate partner violence, domestic abuse, or relationship abuse—is a "pattern of behaviors used by one partner to maintain power and control over another partner in an intimate relationship."[8] In the United States, ten million people are physically abused by their partners each

7. In this piece, I refer to people who experience abuse as "survivors." Advocates and service providers generally prefer the term "survivors" because it conveys more empowerment than the term "victims." *See, e.g.*, *The Survivor's Handbook*, WOMEN'S AID, https://www.womensaid.org.uk/the-survivors-handbook [https://perma.cc/TXY8-X6BV]; SEXUAL ASSAULT KIT INITIATIVE (SAKI), RTI INTERNATIONAL, VICTIM OR SURVIVOR: TERMINOLOGY FROM INVESTIGATION THROUGH PROSECUTION, https://sakitta.org/toolkit/docs/Victim-or-Survivor-Terminology-from-Investigation-Through-Prosecution.pdf [https://perma.cc/QW39-TG36]. However, "victim" is useful in legal contexts, and each individual has their own preference. SAKI, *supra*. Some sources quoted in this piece refer to "victims," and I do not edit their original language. I also still use "victim-blaming" because it is the formal term.

8. *Understand Relationship Abuse: Abuse Defined*, NAT'L DOMESTIC VIOLENCE HOTLINE, https://www.thehotline.org/is-this-abuse/abuse-defined/ [https://perma.cc/W2J6-9BBF]. This Note relies on the national definition of domestic violence, which does not include family violence such as child abuse, elder abuse, or other non-intimate partner violence.

year;[9] globally, 243 million women and girls suffered physical or sexual violence from their partners between 2019 and 2020.[10] Not surprisingly, this has led to characterizations of domestic violence as an American "epidemic" and a global "pandemic."[11] While these statistics highlight physical abuse, domestic violence is now understood as an ongoing system of "coercive control" rather than as discrete incidents of physical assault.[12] The Power and Control Wheel, developed by the Domestic Abuse Intervention Programs in Duluth, Minnesota, shows that domestic violence is perpetrated through various behaviors including coercion and threats, sexual abuse, economic abuse, exploiting male privilege, the use of children, minimizing/denying/blaming, isolation, emotional abuse, and intimidation.[13] Over 90 percent of partner violence does not result in physical injuries as coercive control remains "invisible."[14]

One defining aspect of domestic violence is its gender asymmetry.[15] There is a direct relationship between the severity of the assault and gender asymmetry: as the assault gets more serious, the rates become more gendered.[16] Women in the United States are more likely than men to be raped, physically assaulted, and stalked, and they are more likely to suffer injuries from that abuse.[17] Additionally, domestic violence homicide is mostly male-perpetrated and is the single largest category of causes of female homicide in the United States.[18]

There are various predictors of physical abuse. First, separations (including attempted separations) can trigger additional violence and "revictimiz[ation]."[19] Indeed, a high percentage of U.S. women are killed after they recently separated

---

9. *See* INT'L ASS'N OF CHIEFS OF POLICE, INTIMATE PARTNER VIOLENCE RESPONSE POLICY AND TRAINING GUIDELINES 4 (2017), https://www.theiacp.org/sites/default/files/all/i-j/IACPIntimatePartnerViolenceResponsePolicyandTrainingGuidelines2017.pdf [https://perma.cc/7FGN-D4K2].

10. Phumzile Mlambo-Ngcuka, *Violence Against Women and Girls: The Shadow Pandemic*, UN WOMEN (Apr. 6, 2020), https://www.unwomen.org/en/news/stories/2020/4/statement-ed-phumzile-violence-against-women-during-pandemic [https://perma.cc/HU4K-DS9F].

11. INT'L ASS'N OF CHIEFS OF POLICE, *supra* note 9, at 4.

12. Psychologist Evan Stark first penned the concept of coercive control. EVAN STARK, COERCIVE CONTROL: THE ENTRAPMENT OF WOMEN IN PERSONAL LIFE (2007).

13. DOMESTIC ABUSE INTERVENTION PROGRAMS, POWER AND CONTROL WHEEL (2017), https://www.theduluthmodel.org/wp-content/uploads/2017/03/PowerandControl.pdf [https://perma.cc/3JJR-8WZD].

14. Evan Stark & Marianne Hester, *Coercive Control: Update and Review*, 25 VIOLENCE AGAINST WOMEN 81, 83–84 (2019).

15. This Note uses gendered pronouns, sometimes referring to abusers as "he" and survivors as "she." This choice is intended to highlight the frequency of male-perpetrated violence against female survivors. However, domestic violence is committed by and against individuals of all gender identities.

16. Molly Dragiewicz & Yvonne Lindgren, *The Gendered Nature of Domestic Violence: Statistical Data for Lawyers Considering Equal Protection Analysis*, 17 AM. U. J. GENDER SOC. POL'Y & L. 229, 256 (2009).

17. *Id.* at 258.

18. *Id.* at 248. For discussion of evidence that IoT-facilitated abuse may be exacerbating the gendered nature of domestic violence, see *infra* Part II.

19. Jane K. Stoever, *Enjoining Abuse: The Case for Indefinite Domestic Violence Protection Orders*, 67 VAND. L. REV. 1015, 1025 (2014).

or planned to separate from their abusers, and they are most likely to be murdered in the first few weeks after leaving than at any other time.[20] Second, stalking is strongly associated with physical violence.[21] The U.S. Department of Justice defines stalking as "a course of conduct directed at a specific person that involves repeated visual or physical proximity, non-consensual communication, or verbal, written, or implied threats, or a combination thereof, that would cause a reasonable person fear."[22] It refers to behaviors such as following a person, appearing at their home or work, or leaving written messages or objects.[23] Eighty-one percent of individuals in the United States stalked by a former or current intimate partner experienced physical assault during their relationship.[24] And after the relationship ends, men who stalk their partners are four times more likely to assault them and six times more likely to rape them.[25] In addition, abusers who stalk pose the highest lethality risk.[26]

The United States has made great progress in combatting domestic violence over the past thirty years.[27] For example, we now understand that domestic violence is the leading cause of injury to women, that a huge proportion of women will experience domestic violence, and that domestic violence is not simply about physical violence but rather a broader pattern of power and control.[28] Additionally, there have been criminal and legal reforms at the state and federal levels aimed at increasing sanctions against perpetrators.[29] In recent years, however, researchers, advocates, and service providers have begun to focus on how technology alters understandings of domestic violence and how it complicates current remedies under state and federal laws.

---

20. Brenda Baddam, Note, *Technology and Its Danger to Domestic Violence Victims: How Did He Find Me?*, 28 ALB. L.J SCI. & TECH. 73, 74 (2017).

21. King-Ries, *supra* note 2, at 136.

22. PATRICIA TJADEN & NANCY THOENNES, NAT'L INST. OF JUST., U.S. DEP'T OF JUST., NCJ 169592, STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY 2 (1998), https://www.ncjrs.gov/pdffiles/169592.pdf [https://perma.cc/23AE-XWNR]; *see also Stalking/Cyberstalking*, NAT'L NETWORK TO END DOMESTIC VIOLENCE WOMENSLAW.ORG, https://www.womenslaw.org/about-abuse/forms-abuse/stalkingcyberstalking [https://perma.cc/M9UD-4Y7X] (explaining that the conduct of stalking may be perpetrated by anyone, but is most often committed by a current or former intimate partner).

23. Aily Shimizu, *Domestic Violence in the Digital Age: Towards the Creation of a Comprehensive Cyberstalking Statute*, 28 BERKELEY J. GENDER L. & JUST. 116, 117 (2013).

24. *Id.*

25. Dragiewicz & Lindgren, *supra* note 16, at 254.

26. Baddam, *supra* note 20, at 74; *see also* JACQUELYN C. CAMPBELL, DANGER ASSESSMENT (2019 update), https://www.dangerassessment.org/uploads/DA_NewScoring_2019.pdf [https://perma.cc/BRU9-8SVU] (considering a survivor's being followed, spied on, or left threatening messages as factors associated with increased risk of homicide). Both the separation-assault phenomenon and the link between stalking and physical assault implicate IoT-facilitated abuse because disconnecting devices is similar to "separation," and IoT devices can be tools for stalking. *See infra* Part II.

27. King-Ries, *supra* note 2, at 131.

28. *Id.* at 134–35.

29. *Id.*

B. Technology-Facilitated Domestic Violence

There are numerous terms for technology-facilitated domestic violence. For example, some use "cyber-violence."[30] Recently, scholars proposed the term "technology-facilitated coercive control" to encompass the technological and relational aspects of patterns of abuse against intimate partners;[31] "digital coercive control" also achieves this purpose.[32] Others shorten "technology-facilitated abuse" to "tech abuse,"[33] which this Note uses for consistency. Regardless of the term used, those studying the issue agree that technology has created and continues to create new and greater opportunities to monitor and control survivors, magnifying the harms of domestic violence.[34]

Tech abuse has become a common issue for survivors of domestic violence. The term encompasses the various ways in which abusers can manipulate technology to harass and control individuals, including through emotional manipulation and coercive offenses.[35] It also includes abuse over social media and the dissemination of intimate images without consent, colloquially called "revenge porn."[36] These tactics are not new; rather, technology makes them "easier to employ and considerably less time consuming."[37] It is also important to note that these tactics often occur alongside more traditional forms of abuse.[38]

Two common tactics of tech abuse are location tracking and cyberstalking. Location tracking devices are widespread and easily manipulated as tools for tech abuse.[39] Abusers can monitor survivors using the family-locator function offered by their phone providers' family plan, the location functionality in a phone's operating system, a freestanding GPS device, or even a stalking app sold

30. Hadeel Al-Alosi, *Cyber-Violence: Digital Abuse in the Context of Domestic Violence*, 40 U. NEW S. WALES L.J. 1573, 1573 (2017).

31. BWJP, *Domestic Violence and Technology: New International Research and Resources for Practice*, at 3:40–:45, VIMEO (Oct. 9, 2019), https://vimeo.com/365803650 [https://perma.cc/6BS6-KFZ7] (presentation by Molly Dragiewicz and Bridget Harris); *see also* Molly Dragiewicz, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock & Bridget Harris, *Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms*, 18 FEMINIST MEDIA STUD. 609 (2018).

32. Bridget A. Harris & Delanie Woodlock, *Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies*, 59 BRIT. J. CRIMINOLOGY 530, 530 (2019).

33. *See, e.g.*, Lopez-Neira et al., *supra* note 5, at 23.

34. King-Ries, *supra* note 2, at 138; Baddam, *supra* note 20, at 77.

35. Lopez-Neira et al., *supra* note 5, at 23.

36. Al-Alosi, *supra* note 30, at 1585–86, 1590.

37. *Abuse Goes Digital*, RES. CTR. NEWSLETTER (Res. Ctr. on Domestic Violence: Child Prot. & Custody, Reno, Nev.), Oct. 2019, https://www.rcdvcpc.org/images/blog/201910_-_Technology_Abuse.pdf [https://perma.cc/ZU6C-6XC2].

38. Harris & Woodlock, *supra* note 32, at 532.

39. *See, e.g.*, Reis Thebault, *A Woman's Stalker Used an App that Allowed Him to Stop, Start and Track Her Car*, WASH. POST (Nov. 6, 2019, 11:40 PM), https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/ [https://perma.cc/MFW4-XJVX] (discussing that location-tracking technologies are becoming more common and mentioning a widespread "stalkerware surveillance market" for spyware trackers).

in the App Store.[40] Apple's Find My iPhone feature provides real-time location updates stored in iCloud or an online account, which the abuser can manage and exploit.[41] Stalking apps are nearly undetectable and allow an abuser to see the survivor's location, read texts remotely, see call history, listen to phone calls, or use the phone as a listening device.[42] Attempting to address these stalking apps, in 2015, senators from seven states sponsored the federal Location Privacy Protection Act of 2015, which would (1) require companies to get users' permission before collecting and sharing location data, (2) require companies to inform users how they can stop the collection of such information, and (3) completely ban the development, operation, and sale of GPS stalking apps and establish an Anti-Stalking Fund at the Department of Justice.[43] Critics, including representatives of the mobile advertising industry, argued that the Act would stifle legitimate uses of location tracking such as tracking stolen cars, finding runaway children, and helping people who have Alzheimer's.[44] As of this Note's publication, the legislature has not taken further action on the bill.[45]

In addition to the use of location-tracking devices, cyberstalking is another common form of tech abuse. Cyberstalking is a term for stalking and harassing that occurs in an online environment through the use of the internet, email, or other electronic communication devices.[46] Examples of common cyberstalking behaviors include making unwanted phone calls, sending unsolicited emails, and posting information about the survivor on the internet.[47] According to researchers, up to 50 percent of abusive partners use some form of electronic surveillance for stalking.[48]

Technology increases the risk of domestic violence. First, it allows abusers to overcome geographic and spatial boundaries that would have otherwise prevented them from contacting survivors.[49] The hazards of this "spaceless violence" are severe: when the concept of safety has no clear boundaries, it deters

40. Baddam, *supra* note 20, at 78.

41. *Id.* at 80.

42. *Id.* at 82.

43. S.2270, 114th Cong. (2015). The first iteration of the bill was introduced in 2014. Location Privacy Protection Act of 2014, S. 2171, 113th Cong. The Vice President of NNEDV, Cindy Southworth, testified at the hearing regarding the importance of location privacy and of transparency for domestic violence survivors. *See Location Privacy Protection Act of 2014: Hearing Before the Subcomm. on Privacy, Tech., & the L. of the S. Comm. on the Judiciary*, 113th Cong. 24–33 (2014) (statement of Cindy Southworth, Vice President of Development and Innovation, NNEDV).

44. Baddam, *supra* note 20, at 88.

45. S.2270 - Location Privacy Protection Act of 2015, CONGRESS.GOV https://www.congress.gov/bill/114th-congress/senate-bill/2270 [https://perma.cc/46F5-R67F].

46. Al-Alosi, *supra* note 30, at 1582; Shimizu, *supra* note 23, at 117.

47. SHANNAN CATALANO, BUREAU OF JUST. STATS., U.S. DEPARTMENT OF JUST., NCJ 224527, STALKING VICTIMS IN THE UNITED STATES – REVISED 1 (2012), https://www.bjs.gov/content/pub/pdf/svus_rev.pdf [https://perma.cc/4QFA-DQWR].

48. Baddam, *supra* note 20, at 83.

49. Al-Alosi, *supra* note 30, at 1578.

women from leaving and jeopardizes their ability to protect themselves.[50] For example, a survivor may choose not to risk escaping if she knows the abuser will be able to track her to the new location.

Another hazard is psychological, because technology allows abusers to create "a sense of omnipresence" that erodes survivors' feelings of safety, even after separation.[51] For example, physical and sexual abuse require the abuser to be present with the survivor, so she may feel safer once she is able to move to a shelter or otherwise escape. On the other hand, a survivor of tech abuse feels endangered no matter where she is, because the threats and surveillance are one-sided and undetectable—that is, even if she cannot see her abuser, she knows he could be watching. In addition, the growing prevalence and ease of technology mean abusers can commit this spaceless violence without any advanced computing skills. Indeed, the GPS tracking devices and stalking phone apps discussed previously show that tech abuse can be both technologically simple and inexpensive.[52]

Further, society's dependence on technology shows no signs of slowing, which may create greater problems in the future. Andrew King-Ries, for one, has argued that teenagers' use of technology may undermine our progress in addressing cyberstalking.[53] He has argued that teenagers' incorporation of technology into their personal lives has reduced their expectations of privacy in intimate relationships, normalizing a "boundarylessness" which may make teenage survivors more accepting of abusive behaviors by partners.[54] For example, constant connectivity can blur individual boundaries and create a sense of entitlement to information about the other person's location, activities, and acquaintances.[55] There is reason to worry because, as teens may carry these unhealthy relationship patterns into adulthood, we risk creating a "new generation of domestic violence batterers"[56] and survivors. Accordingly, the combination of our increasing dependence on technology and the fast-paced development of new technologies warrants immediate attention.

---

50. Harris & Woodlock, *supra* note 32, at 538.

51. Al-Alosi, *supra* note 30, at 1578.

52. *See id.* at 1573; Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart & Nicola Dell, *"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology*, 2018 Proc. CHI Conf. on Hum. Factors in Computing Sys., no. 1, at 1, 9.

53. King-Ries*, supra* note 2, at 131.

54. *Id.* at 132.

55. *Id.* at 157.

56. *Id.* at 154.

II.
THE INTERNET OF THINGS AND DOMESTIC VIOLENCE

A. What is the Internet of Things?

The Internet of Things (IoT) is an umbrella term describing the network of standalone internet-connected devices that individuals can monitor or control from a remote location.[57] IoT devices are "smart" because of how they share data, allowing them to communicate with other devices through apps or websites, and with each other when connected on shared networks.[58] Most of these devices can connect to multiple devices at the same time.[59] For example, if a person's lighting system is IoT-connected, they can control the lights remotely through their smartphone or other internet-connected devices rather than with a physical switch.[60] Some major companies involved in making IoT technologies include Microsoft, Amazon, Google, AT&T, and Fitbit.[61] IoT devices are prevalent and encompass a range of technologies such as smart appliances (speakers, refrigerators, TVs), personal devices (toys, watches, health trackers, medical devices, glasses, cars), home systems (thermostats, security cameras, doorbells, lighting), home assistants (Amazon Alexa, Google Nest), and more.[62] As the IoT grows, additional devices will join that list. Indeed, research anticipates high rates of growth: a 2017 McKinsey report stated that 29 million homes in the United States had smart technology and that the number was growing by 31 percent each year;[63] Business Insider estimated that the number of IoT-enabled devices worldwide will increase 12 percent annually, from 27 billion in 2017 to 125 billion in 2030.[64]

As devices become increasingly connected due to the IoT, consumers and businesses alike have voiced concerns regarding privacy and security issues such as massive data generation that leaves sensitive information vulnerable to hackers and unwanted data collection by technology companies.[65] What they have paid less attention to, however, are the privacy, security, and safety risks for survivors of domestic violence specifically. Even if designers of IoT devices

---

57. Meola, *supra* note 6.

58. *Internet of Things (IoT)*, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://www.techsafety.org/iot-evidence [https://perma.cc/4RZ9-YWYW].

59. *Id.*

60. *See How Do Smart Switches Work*, IDISRUPTED (Jan. 14, 2019), https://idisrupted.com/how-do-smart-light-switches-work/ [https://perma.cc/YB4K-W52V].

61. Meola, *supra* note 6.

62. *See* UNIV. COLL. LONDON, TECH ABUSE (2018), https://www.ucl.ac.uk/steapp/sites/steapp/files/gender-iot-tech-abuse.pdf [https://perma.cc/YJ6L-WMUD]; Lopez-Neira et al., *supra* note 5, at 22, 23.

63. John Naughton, Opinion, *The Internet of Things Has Opened Up a New Frontier of Domestic Abuse*, GUARDIAN (July 1, 2018, 2:00 AM), https://www.theguardian.com/commentisfree/2018/jul/01/smart-home-devices-internet-of-things-domestic-abuse [https://perma.cc/N5VQ-XLLR].

64. Meola, *supra* note 6.

65. *Id.*

added security features to decrease vulnerability to hackers or data collection, the devices still assume that all users *within* a home trust each other to use the devices properly.[66] But in homes where intimate partner violence occurs, this assumption allows abusers to misuse certain features to monitor, harass, threaten, and isolate survivors.[67]

B. IoT-Facilitated Abuse as Domestic Violence

There are limited statistics on the frequency of IoT-facilitated abuse, but both empirical research and anecdotal evidence make clear that IoT-facilitated abuse is occurring. Between 2017 and 2018, a group of researchers from University College London conducted a six-month feasibility study into whether IoT devices could be manipulated into instruments of abuse.[68] The study concluded that IoT-facilitated abuse was not yet widespread, but that the devices' data flows, configurations, and settings showed "potential for exploitation."[69] One lead researcher stated that the study aimed to "proactively highlight" opportunities for abuse such that advocates and government actors would not be left reacting to issues only after they arose.[70]

In 2018, the *New York Times* conducted more than thirty interviews with survivors, lawyers, shelter workers, and emergency responders regarding the prevalence of IoT-facilitated abuse.[71] The investigation revealed that survivors were experiencing dystopian activity such as air conditioners being remotely switched off, digital front door passcodes being changed every day, and doorbells ringing incessantly without anyone being outside.[72] Legal scholars described additional tactics such as changing the temperature in a home from miles away, or boiling a kettle of water to remind the survivor that the abuser was watching.[73] A BBC journalist added that abusers could use smart sensors on doors to check when the survivor left the house; control smart locks to restrict the survivor's ability to leave the house; and monitor the search history of voice-

66. UNIV. COLL. LONDON, *supra* note 62; Lopez-Neira et al., *supra* note 5, at 23.

67. *Internet of Things (IoT)*, *supra* note 58.

68 For more information about the project's plan and outcomes, see *Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse*, UNIV. COLL. LONDON, https://www.ucl.ac.uk/research/domains/collaborative-social-science/social-science-plus/IOT-and-domestic-violence [https://perma.cc/PM2Z-ZZ7W].

69. Heidi Vella, *IoT Devices and Smart Domestic Abuse: Who Has the Controls?*, E&T MAG. (June 20, 2018), https://eandt.theiet.org/content/articles/2018/06/iot-devices-and-smart-domestic-abuse-who-has-the-controls [https://perma.cc/4AJ9-J28M].

70. *Id.* (quoting Dr. Leonie Tanczer).

71. Nellie Bowles, *Thermostats, Locks, and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html [https://perma.cc/BWS9-T5S2].

72. *Id.*

73. Lopez-Neira et al., *supra* note 5, at 25.

controlled virtual assistants to make sure the survivor was not seeking help.[74] Within a relationship, the fact that one person is the account administrator for all IoT devices in the home is a tactic to create dependence.[75] After the relationship ends, IoT-facilitated abuse continues to enforce coercive control through remote-controlled harassment, monitoring, and intimidation.

One of the first documented court cases involving IoT-facilitated abuse occurred in May 2018. In that case, a couple in the United Kingdom had initially installed a smart-home system together so they could access their lighting, heating, and alarm system remotely.[76] After the couple split up, the abuser hacked into the wall-mounted iPad to spy on his estranged wife and logged into the iPad's audio facility through a mobile app to listen to her conversations.[77] Although court cases regarding IoT-facilitated abuse remain rare compared to informal reports to domestic violence shelters and help lines, it is likely that incidents will increasingly reach U.S. courts as IoT devices become more prevalent.

C. Unique Characteristics and Harms of IoT-Facilitated Abuse

IoT-facilitated abuse has unique characteristics that exacerbate other forms of tech abuse and produce new harms. These harms include magnifying the gendered nature of domestic violence; causing jurisdictional, evidentiary, and constitutional confusion; allowing abusers to circumvent geographic boundaries; and creating unique forms of victim-blaming and minimization.

Like domestic violence generally, IoT-facilitated abuse is a gendered offense: most survivors are women and most abusers are men.[78] According to John Naughton, men still buy and install most networked devices—thus, these men will know the passwords, and the survivors will be unable to change them.[79] Even if men did not set up the devices, former and current partners, spouses, and cohabitants typically have unique "access to and knowledge about" each other, which means the abuser might already know the survivor's passwords or will have a greater chance at guessing them.[80] In addition, the abuser may have insisted that his partner share her passwords with him during the relationship.[81] In sum, IoT-facilitated abuse may be even more gendered than domestic violence

74. Alex Riley, *How Your Smart Home Devices Can Be Turned Against You*, BBC FUTURE (May 11, 2020), https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse [https://perma.cc/8M8K-HE9W].

75. *Id.*

76. *Jealous Husband Used Wall-Mounted iPad in his 'Smart Home' to Spy on Estranged Wife, Court Hears*, TELEGRAPH (May 10, 2018, 3:20 PM), https://www.telegraph.co.uk/news/2018/05/10/smart-home-stalker-jealous-husband-used-wall-mounted-ipad-heating/ [https://perma.cc/LN4A-AG2J].

77. *Id.*

78. Naughton, *supra* note 63.

79. *Id.*

80. *See* Thebault, *supra* note 39.

81. Freed et al., *supra* note 52, at 6.

generally because men often purchase and set up IoT devices, giving them control over the tools of abuse.

The legal implications of IoT-facilitated abuse include jurisdictional, evidentiary, and constitutional issues. First, it can be difficult to determine the jurisdiction in which a survivor can pursue a civil suit against an abuser who misuses technology because cyberspace has no territorial borders.[82] This especially applies to IoT-facilitated abuse, because the devices are specifically designed to be controlled via technology when the user is *not* near the device.[83] Fortunately, some courts have taken expansive views of jurisdiction in cases involving technology. For example, the California Court of Appeal for the Third District held in 2017 that if a person in another state commits an act of domestic violence against someone in California using social media or electronic communications, California courts have jurisdiction to issue a restraining order.[84]

In addition to jurisdictional issues, it can be difficult to collect evidence of IoT-facilitated abuse.[85] The NNEDV suggests that survivors document suspicious activity on their accounts such as password changes, and track strange activity in real time by taking videos or recordings.[86] Another option would be for police and prosecutors to publish lists of what evidence is necessary to investigate or prosecute IoT-facilitated abuse. This would allow advocates to work with survivors to document the necessary information for an incident report. However, because IoT-facilitated abuse is nonphysical, evidence of abusive conduct may only exist in records on the abuser's device, records of the abuser's online activity, or other records that are difficult for the survivor to obtain. If law enforcement is unable to easily access the abuser's digital information, it may choose to rely on the survivor's data instead. Thus, a survivor who makes a police report may be subject to intrusive investigations in which law enforcement compounds the invasion of her digital privacy. And even if the survivor agrees, many police departments do not actually have the resources and training in computer technology to conduct investigations of cybercrimes.[87]

Finally, any attempts to regulate the decentralized internet must be narrow enough to avoid violating the First Amendment right to freedom of speech. The Supreme Court's First Amendment jurisprudence generally protects speech, making narrow exceptions for "true threats"[88] and "speech integral to criminal

82. Shimizu, *supra* note 23, at 129–30.

83. *See* Meola, *supra* note 6 (describing how remote-control capabilities are a defining feature of IoT devices).

84. Hogue v. Hogue, 224 Cal. Rptr. 3d 651 (2017) (vacating order quashing service on estranged husband who after a history of physical abuse posted a mock suicide video on his wife's Facebook page, leading her to petition for a restraining order).

85. *See, e.g.*, *Internet of Things (IoT)*, *supra* note 58.

86. *Id.*

87. King-Ries, *supra* note 2, at 142.

88. Virginia v. Black, 538 U.S. 343, 359 (2003).

conduct."[89] Courts do enforce these exceptions in the domestic violence context. For instance, the Ninth Circuit upheld a conviction under the Interstate Stalking Punishment and Prevention Act where the defendant's harassing conduct occurred over text message and email.[90] Responding to the defendant's First Amendment challenge, the court held that "any expressive aspects" of his communications were "integral to criminal conduct" as defined in the stalking statute and thus not afforded protection.[91] In a case involving IoT devices, an additional complexity is that communication between an IoT device and its user is still a novel technology. While courts have held that phone calls, text messages, emails, and website postings can constitute speech,[92] a survivor could argue that IoT-facilitated abuse does not qualify for First Amendment protection because a user's manipulation of an IoT device through verbal or nonverbal conduct is not speech.

Beyond unique legal implications, IoT-facilitated abuse causes unique harms to survivors. Tech abuse already endangers survivors by blurring geographic and spatial boundaries, allowing abusers to harass from a distance, and deterring survivors from leaving abusive situations because they feel they cannot escape.[93] IoT-facilitated abuse makes this barrier to safety even harder to overcome. Because of the paranormal-like nature of the activity, survivors feel like they are "losing control of their [own] home" and being followed at all times.[94] Unlike with other forms of tech abuse, survivors of IoT-facilitated abuse do not need to open their text messages or log into their computers to feel unsafe. Instead, the perpetrator's control extends to all corners of the home, and the abuser can use these tactics at any time. Indeed, one survivor described her abuse as "jungle warfare" because she had no idea where the attacks were coming from.[95]

In addition to this psychological fear, survivors know that society will not always believe them if they share their experiences and may criticize them instead. IoT-facilitated abuse engenders a distinct form of victim-blaming—a phenomenon that is already highly common. In the popular understanding of domestic violence, an attitude of victim-blaming suggests that the survivor, rather than the perpetrator, bears responsibility for abuse. One myth is that

89. United States v. Alvarez, 567 U.S. 709, 717 (2012) (citations omitted).

90. United States v. Osinger, 753 F.3d 939, 940–42 (9th Cir. 2014). For further discussion of the Interstate Stalking Punishment and Prevention Act, see *infra* notes 169–171 and accompanying text.

91. *Id.* at 947 (citation omitted).

92. *See, e.g.*, *id.* (text messages and emails); United States v. Petrovic, 701 F.3d 849, 852–56 (8th Cir. 2012) (text messages and a website); United States v. Shrader, No. 1:09–0270, 2010 WL 2179572, at *1 & n.1, *4–5 (S.D. W. Va. Apr. 7, 2010) (magistrate report and recommendation), *adopted*, 2010 WL 2179570 (S.D. W. Va. May 26, 2010), *aff'd*, 675 F.3d 300 (4th Cir. 2012) (phone calls).

93. Shimizu, *supra* note 23, at 118; Al-Alosi, *supra* note 30, at 1578; Harris & Woodlock, *supra* note 32, at 538.

94. Bowles, *supra* note 71.

95. *Id.*

individuals who stay in relationships with abusive partners are either lying about experiencing abuse or responsible for their own abuse by choosing to stay.[96] This myth fails to consider the multitude of barriers to leaving.[97] Victim-blaming in tech abuse situations typically involves the false perception that survivors are responsible for the abuse because they failed to stop using the exploited technology.[98] In cases of IoT-facilitated abuse, victim-blaming might manifest as blaming survivors for sharing too much personal information that could enable others to compromise their accounts or devices, or for being too eager to purchase new technologies without considering the associated risks.

The results of victim-blaming in IoT-facilitated abuse cases are emotionally damaging and dangerous. First, telling a survivor of IoT-facilitated abuse that she should not have purchased the technology would be both inaccurate and unhelpful if she was not the one who purchased it. As discussed previously, the abuser could have purchased and installed the IoT devices,[99] then purposefully registered the devices under his own name. This is further complicated by the fact that the survivor might still be financially dependent on or living with the abuser at the time she seeks help.[100]

Second, even if the survivor chose to install the networked devices on her own, any advice to simply stop using the devices and "get offline" fails to address the root cause of abuse and can also create more dangers for the survivor.[101] In cases of tech abuse more generally, telling survivors to stop using technology fails to recognize that technology can be a source of "comfort and assistance."[102] Technology can help decrease isolation (which is a tactic of abuse) by connecting survivors with their friends and family.[103] In addition, disengaging from technology prevents survivors from seeking general aid, including by calling 911 during an emergency or contacting professionals such as doctors, therapists, and lawyers.[104] In the case of IoT-facilitated abuse, advice to "get offline" forces survivors to trade their access to devices that make their lives feel more connected for the potential minimization of risk. It also ignores the fact that survivors deserve an opportunity to use those same devices in proper ways to

96. *Challenging the Myths*, WOMEN'S AID, https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/myths/ [https://perma.cc/M2G7-68AG]; *see also Why People Stay*, NAT'L DOMESTIC VIOLENCE HOTLINE, https://www.thehotline.org/is-this-abuse/why-do-people-stay-in-abusive-relationships/ [https://perma.cc/K9LX-XBZ9] (discussing how asking survivors "why" they do not leave or "why" they stay implies that they had a real choice between leaving and staying).

97. Barriers include financial dependency, fear or shame, cultural and language barriers, children, and more. *Id.*

98. Harris & Woodlock, *supra* note 32, at 539.

99. *See* Naughton, *supra* note 63 (stating that men purchase and install the majority of IoT devices).

100. *See Why People Stay*, *supra* note 96.

101. Harris & Woodlock, *supra* note 32, at 540.

102. *Id.*

103. *Id.*

104. Baddam, *supra* note 20, at 80–81.

increase their own safety (e.g., by installing a video doorbell to check whether the abuser is at the door). Ultimately, victim-blaming attitudes put the responsibility on survivors to change their behavior in order to avoid abuse. Instead of creating conditions that enable them to be free from violence, survivors have to do the "safety work" of protecting themselves.[105]

Related to victim-blaming, IoT-facilitated abuse also leads to a unique form of minimization. "Minimizing, denying, and blaming" and "emotional abuse" are common abusive behaviors found on the Power and Control Wheel.[106] They include playing mind games and making the survivor think she is not mentally stable.[107] Gaslighting is a form of emotional abuse that occurs when the perpetrator manipulates a person to doubt her own perception of reality and question her own sanity.[108] The abuser does this gradually through tactics such as withholding (pretending not to understand), countering (questioning the accuracy of the survivor's memory), diverting (changing the subject), trivializing (making the survivor's feelings or concerns seem unimportant), and forgetting (pretending to forget what happened, or denying that it happened).[109]

As advocates continuously stress, abusers may perpetrate abuse with new technology, but it still involves old and common behaviors.[110] The ability to control IoT devices remotely likely makes it easier for an abusive partner to employ gaslighting techniques. For instance, it would be difficult for an abuser to send a message from his phone to the survivor's phone and then claim he did not do it. But it would be plausible for an abuser who turns the volume up to deafening levels at the survivor's house to claim that he did so accidentally. In addition, if the survivor experiences strange incidents of ringing doorbells and flickering lights but does not document evidence, the abuser could claim that the survivor was imagining things and damage her credibility. Studies show that victim-blaming in tech abuse often deters women from seeking help because they are made to feel ashamed and afraid that they will not be believed.[111] Victim-blaming in IoT-facilitated abuse has a similar negative effect.

---

105. Harris & Woodlock, *supra* note 32, at 540.

106. DOMESTIC ABUSE INTERVENTION PROGRAMS, *supra* note 13.

107. *Id.*

108. *See What is Gaslighting?*, NAT'L DOMESTIC VIOLENCE HOTLINE (May 19, 2014), https://www.thehotline.org/2014/05/29/what-is-gaslighting/ [https://perma.cc/K6XC-PHG7]. The term comes from a 1938 play called *Gas Light* in which a husband attempts to drive his wife crazy by dimming the lights in their home and then denying that the light changed when his wife points it out. *Id.* The play was adapted into a movie starring Charles Boyer and Ingrid Bergman. GASLIGHT (Metro-Goldwyn-Mayer 1944).

109. *What is Gaslighting?*, *supra* note 108.

110. *See* Thebault, *supra* note 39 ("What we know, what we've always known, is that abusers and perpetrators will use any tactic and tool they can access in order to perpetrate harassment and abuse. . . . These are modern forms of old tactics and behaviors." (quoting Erica Olsen, director of NNEDV's Safety Net Project)).

111. Harris & Woodlock, *supra* note 32, at 539.

Minimization is not only an abuser's tactic. Often law enforcement engages in minimization by turning a blind eye to tech abuse—either consciously or not. According to a newsletter for prosecutors, abusers who utilize technology believe they can get away with the abuse because it is hard to prove or because there are no laws against what they are doing.[112] Unfortunately, the actions of police sometimes support this viewpoint. For example, survivors of cyberstalking have been told by police to "[c]all us if he shows up."[113] This minimizes the survivor's fear caused by harassment and monitoring and implies that physicality is necessary for abuse to be "real." The physicality requirement may also reinforce classism because wealthy men engage in the same tactics of domestic violence as other men but have greater access to technologies that help conceal the abuse.[114] Law enforcement's minimization of nonphysical abuse suggests that the state is not interested in regulating and condemning technologically advanced forms of violence. Indeed, in the case of IoT-facilitated abuse, a physicality requirement would nullify almost all complaints to police.

In addition, although controlling behaviors such as stalking are abusive in and of themselves and strongly linked to future physical violence, the breach of stalking provisions in a restraining order is not taken as seriously as actual physical offenses such as assault.[115] Similarly, the breach of protection orders using digital means is regarded as a "low-level risk[]."[116] Thus, it would be unsurprising for police to take violations of protection orders prohibiting contact or monitoring through IoT devices less seriously, as compared to physical stalking or the usage of more familiar digital tools such as GPS tracking or online threats.

IoT-facilitated abuse not only causes psychological and emotional abuse, but also may facilitate physical violence. As discussed in Part I, stalking and separation are correlated with physical violence. A 2002 study found that 68 percent of femicide[117] victims and attempted femicide survivors experienced

112. Jane Anderson & Kaofeng Lee, *The Internet & Intimate Partner Violence: Technology Changes, Abuse Doesn't*, STRATEGIES (AEquitas, Washington, D.C.), Jan. 2017, at 1, 4, https://aequitasresource.org/wp-content/uploads/2018/09/The-Internet-and-Intimate-Partner-Violence-Technology-Changes-Abuse-Does-Not-Issue16.pdf [https://perma.cc/D94J-TB2W].

113. *Id.*

114. *See* Bowles, *supra* note 71. Many of the women from *The New York Times* investigation came "from wealthy enclaves where [smart] technology has taken off." *Id.* It is likely that, when the law requires physical abuse, wealthy abusers who have greater access to technology may escape accountability for controlling, monitoring, and harassing survivors while less wealthy abusers cannot.

115. Al-Alosi, *supra* note 30, at 1593.

116. Harris & Woodlock, *supra* note 32, at 541.

117. The World Health Organization (WHO) defines "femicide" as "the murder of a woman" because she is a woman. WORLD HEALTH ORGANIZATION, UNDERSTANDING AND ADDRESSING VIOLENCE AGAINST WOMEN: FEMICIDE 1 (2012), https://apps.who.int/iris/bitstream/handle/10665/77421/WHO_RHR_12.38_eng.pdf [https://perma.cc/6QUW-52KH]. The definition is broad and includes both intimate femicide and non-intimate femicide, but the WHO notes that a large proportion of femicides are committed by current or former partners from violent relationships. *Id.*

stalking in the twelve months before the actual or attempted femicide.[118] The most frequent types of stalking included following or spying, unwanted phone calls, and keeping the survivor under surveillance.[119] Because abusers can use IoT devices as tools to accomplish the same goals as stalking—locating and surveilling survivors—IoT-facilitated abuse likely implicates the same dangers associated with stalking, including death. Moreover, an Australian study found that 100 percent of survivors abused by an intimate partner reported that tech abuse began or escalated at separation.[120] Indeed, digital safety experts warn that uninstalling IoT devices or trying to regain control of the accounts can escalate conflict.[121] In this way, IoT abuse makes separation, which is already dangerous for domestic violence survivors, even riskier.[122]

It is important to recognize the unique implications of IoT-facilitated abuse because they impact the remedies for abuse. Several examples may be instructive. First, no civil or criminal laws currently cover abuse through IoT devices.[123] Therefore, a lawyer should be aware of evidentiary or jurisdictional issues before filing a case and should be able to analogize the characteristics of IoT-facilitated abuse to other forms of abuse in order to adequately claim that the existing domestic violence laws apply. Second, even if the laws are applicable, they will be ineffective if we do not combat victim-blaming and minimization. The police officer may choose not to investigate, or the judge may refuse to find the perpetrator in contempt for violating a protection order, if they do not perceive IoT-facilitated abuse as a real harm. Third, awareness of domestic violence is a prerequisite to successful nonlegal remedies. For example, safer IoT design requires an understanding of the device's user base—in this case, an understanding that men buy most IoT devices and men perpetrate domestic violence at higher rates—and a training on digital safety may backfire if the security expert does not understand that disconnecting from compromised

118. Phillip J. Resnick, *Stalking Risk Assessment*, *in* STALKING 61, 71 (Debra A. Pinals ed., 2007).

119. *Id.*

120. M. DRAGIEWICZ, AUSTL. COMMC'NS CONSUMER ACTION NETWORK, TECHNOLOGY AND DOMESTIC VIOLENCE: AUSTRALIAN SURVIVORS' EXPERIENCES (2019), https://accan.org.au/Domestic%20Violence%20and%20Communications%20Technology%20survivor%20exp%20infographic%2020190801.pdf [https://perma.cc/9LHR-8J9V].

121. *See* Bowles, *supra* note 71. This escalation likely occurs because abusers can tell when a device is uninstalled and will feel a loss of control over their victim, and exerting control is their goal in misusing the devices in the first place. Thus, as discussed in Part III, it might be safer for survivors to learn how to safely use such devices and to avail themselves of legal remedies informed by tech abuse, rather than to be asked to disconnect from technology.

122. *See* Stoever, *supra* note 19, and related discussion on the "separation assault" phenomenon.

123. For a discussion of various civil and criminal laws that could be relevant in the context of IoT-facilitated abuse, but that do not explicitly mention IoT devices, see Parts III.B, III.C. IoT device law has slowly started to develop in the area of privacy and cybersecurity, with California being the first state to enact such legislation. Act of Sept. 28, 2018, ch. 860, 2018 Cal. Stat. 5573 (codified at CAL CIV. CODE § 1798.91.04–.06 (West 2020)) (requiring *manufacturers* to equip "connected devices" with certain security features). However, no IoT law currently exists that governs misuse by *abusers*.

devices risks separation assault. Ultimately, the availability and effectiveness of the remedies discussed below depend on our understanding of the unique characteristics and harms of IoT-facilitated abuse.

III.
REMEDIES UNDER CURRENT LAW & SUGGESTIONS FOR CHANGE

As a result of the unique implications of IoT-facilitated abuse, it is critical to use any and all existing remedies for domestic violence in creative ways, and also to open new avenues for addressing IoT-facilitated abuse more directly.

This Note aims to provide a range of remedies, as it operates under the belief that society must make available multiple types of remedies such that survivors may each make their own informed decisions as to which remedy will be most desirable and effective in their unique situations. Remedies serve different functions: preventing abuse in a relationship, deterring abuse more broadly in society, financially compensating the survivor, punishing the perpetrator, and expressing social condemnation of abuse. Not all remedies will work alongside each other, however. For instance, a survivor who wants to remove the perpetrator's access to her devices and also to remain in the relationship will seek different remedies compared to a survivor who prefers that a court sentence her abuser. Remedies also depend on which stage of domestic abuse the survivor is experiencing—that is, whether she is in the relationship and cohabitating with the abusive partner, whether she is preparing to contact the police or seek shelter elsewhere, or whether she has already left and is trying to rebuild her life.[124]

This Section cannot and does not purport to cover all possibilities but aims to explain ways to tackle IoT-facilitated abuse in the following areas: the legal conception of domestic violence, civil remedies, criminal remedies, and nonlegal remedies. It will also highlight potential issues and critique the effectiveness of certain remedies. Broadly, there are two major flaws: (1) current laws, which were not created to address the unique implications of IoT-facilitated abuse, are vulnerable to counterarguments and to judicial discretion as to whether the existing body of domestic violence law applies; and (2) contact with the legal system can be expensive, traumatizing, and even dangerous for survivors and their communities. Therefore, there is a strong need for alternatives. The Section ends by discussing four nonlegal remedies: cultural change, digital safety trainings for survivors, community accountability strategies, and safer design.

124. Charlotte Webb, *What Happens When the Internet of Things Becomes an Accomplice in Domestic Abuse?*, ADOBE XD IDEAS (May 27, 2020), https://xd.adobe.com/ideas/perspectives/social-impact/internet-accomplice-domestic-abuse/ [https://perma.cc/AQ56-4G46] (describing three typical stages of domestic abuse).

A. Expanding the Definition of Domestic Violence

Addressing IoT-facilitated abuse necessitates expanding the legal definition of domestic abuse to explicitly include IoT-facilitated abuse. This change is insufficient as a remedy in and of itself, but is a critical first step because any potential remedy within the legal system is necessarily limited or expanded by this definition.

Currently, the legal system insufficiently addresses the issue of tech abuse. There is evidence that the Trump administration hindered progress toward a broad definition of domestic violence. In 2018, the U.S. Department of Justice Office on Violence Against Women revised its definition of domestic violence to only include harms that would constitute a felony or misdemeanor crime.[125] In contrast, the Obama administration's definition was expansive and explained the various methods of coercive control.[126] Although one could expect the Biden administration to reinstate the Obama-era definition, until that happens, the harms caused by a limited definition of domestic violence will be exacerbated when emerging technologies are involved. For example, if a government attorney or law enforcement official is (1) not aware that networked devices are tools of abuse, (2) not trained to recognize evidence of such abuse, or (3) not permitted to act on what their employer does not define as abuse, the survivor is precluded from seeking otherwise-available remedies.

In a 2015 study on law enforcement responses to domestic violence, the Police Executive Research Forum found that 51 percent of respondent agencies adopted the Obama administration's definition of domestic violence.[127] Although it is unclear to what extent the 2018 revised definition has impacted law enforcement agencies, and there are some positive signs that law enforcement departments are expanding their definitions of domestic violence to include technology, definitions still fail to specifically address IoT-facilitated abuse. For example, the International Association of Chiefs of Police's *Intimate Partner Violence Response Policy and Training Guidelines*, created in 2017, suggest policies to strengthen trainings on domestic violence investigations, including "technology used pre-, during, and post-assault."[128] The *Guidelines* also encourage a victim-centered approach that takes reports of abuse seriously and credits victims' lived experiences,[129] which can be critical when working on tech abuse cases where there is no physical evidence. Similarly, the January 2017

125. Off. on Violence Against Women, *Domestic Violence*, U.S. DEP'T OF JUST., https://www.justice.gov/ovw/domestic-violence [https://perma.cc/SN65-KWY5].

126. Off. on Violence Against Women, *Domestic Violence*, U.S. DEP'T OF JUST., https://web.archive.org/web/20180409111243/https:/www.justice.gov/ovw/domestic-violence.

127. *Police Improve Response to Domestic Violence, but Abuse Often Remains the 'Hidden Crime*,*'* SUBJECT TO DEBATE (Police Exec. Rsch. F., Washington, D.C.), Jan./Feb. 2015, at 1, 2, https://www.policeforum.org/assets/docs/Subject_to_Debate/Debate2015/debate_2015_janfeb.pdf [https://perma.cc/YZY5-FNZH].

128. INT'L ASS'N OF CHIEFS OF POLICE, *supra* note 9, at 8.

129. *Id.*

issue of *Strategies: The Prosecutors' Newsletter on Violence Against Women* informed its readers that tech abuse is one tool that abusers can use to exert power and control over their partners.[130] It gives guidelines on holding abusers accountable (through best practices in retrieving digital evidence, for example), and on working with survivors (documenting and reporting abuse and securing devices).[131] Even though both of these publications illustrate that police and prosecutors understand that domestic violence is about control and can be perpetrated through technology, they fail to address IoT-facilitated abuse specifically and should be updated.

Whether law enforcement officers act upon expanded definitions of domestic violence is not covered in this Section. Evidence of police officers' minimization of nonphysical abuse and their own perpetration of domestic violence (both discussed later in this Note) suggests that enforcement will be an issue. But as a baseline, all local, state, and federal government definitions of domestic violence must explicitly address IoT devices and IoT-facilitated abuse.

B. Civil Remedies

1. Tort Lawsuits for Damages

Domestic violence causes serious harm. Tort law, especially personal injury law, can dictate how and when survivors are compensated for these harms. One benefit of tort law as a vehicle for obtaining a remedy is the availability of financial recovery. Financial recovery can help survivors with their immediate needs and with their longer-term self-sufficiency and safety.[132] In addition, prevailing in a civil suit can give survivors closure and empowerment as well as deter abusers.[133] Some tort law claims, such as a claim for intentional infliction of emotional distress (IIED), offer well-suited remedies for survivors of nonphysical violence.[134] These claims should be used to the extent possible to provide legal recourse for survivors of IoT-facilitated abuse.

Some states recognize an independent tort claim for stalking.[135] California became one of the first states to create a distinct civil action for stalking in 1993 with the enactment of California Civil Code Section 1708.7.[136] In 1998, the legislature expanded the statute to include written and verbal threats made through an "electronic communication device."[137] In 2014, another amendment

130. Anderson & Lee, *supra* note 112, at 8.

131. *Id.* at 1.

132. Camille Carey, *Domestic Violence Torts: Righting a Civil Wrong*, 62 KAN. L. REV. 695, 696 (2014).

133. *Id.*

134. *Id.*

135. Shimizu, *supra* note 23, at 128.

136. Act of Sept. 29, 1993, ch. 582, 1993 Cal. Stat. 2879, § 1 (codified as amended at CAL. CIV. CODE § 1708.7 (West 2020)).

137. Act of Sept. 25, 1998, ch. 825, 1998 Cal. Stat. 5160, § 2.

broadened the statute to include "implied" threats made "directly, indirectly, or through third parties, by any action, method, device, or means."[138] No IoT case has tested Section 1708.7 yet. On one hand, IoT-facilitated abuse likely satisfies the threat element because contact through a "device" is now included. On the other hand, it is clear that legislators did not consider the harms of networked devices. The statute covers conduct intended to "follow, alarm, place under surveillance, or harass" the plaintiff.[139] However, it defines "surveillance" as "remaining present outside of the plaintiff's school, place of employment, vehicle, [or] residence."[140] Thus, the tort of stalking in California excludes surveillance from *inside* the plaintiff's residence. An effective civil stalking statute must cover indirect surveillance and eliminate both the physicality and location requirements.

A claim for intentional infliction of emotional distress applies when an abuser "intentionally or recklessly causes severe emotional harm" through "extreme and outrageous conduct."[141] One obstacle to bringing a successful IIED claim is that the ubiquity of domestic violence makes some behaviors hard to label as "outrageous."[142] Additionally, the "male-dominated judiciary" tends to avoid "private" issues in the home and to value economic and physical security over emotional security.[143] Although most jurisdictions in the United States eliminated spousal immunity for domestic violence by 1988, there is evidence of courts' de facto refusal to abrogate spousal immunity, especially for IIED claims.[144] A survivor of IoT-facilitated abuse who makes an IIED claim may face this barrier. First, IoT devices are not perceived as outrageous—at least not when they are used as intended. In general, connected devices are common and useful gadgets; outrageousness would stem from a user's manipulation of the device and not the device itself. And second, IoT devices are located primarily in private households into which courts often prefer not to probe. Despite its drawbacks, an IIED claim is a unique tort primarily meant to redress emotional injuries, which advocates should leverage to remedy the emotional and psychological harms of IoT-facilitated abuse.

2. Civil Protection Orders

Another remedy under the civil legal system is the civil protection order, also called a domestic violence restraining order (DVRO). DVROs are binding injunctions that a state court issues to enjoin an individual "from engaging in

138. Act of Sept. 30, 2014, ch. 853, 2014 Cal. Stat. 5598, § 1.
139. CAL. CIV. CODE § 1708.7(a)(1).
140. *Id.* § 1708.7(b)(6).
141. Carey, *supra* note 132, at 702.
142. Merle H. Weiner, *Domestic Violence and the Per Se Standard of Outrage*, 54 MD. L. REV. 183, 188 (1995).
143. *Id.* at 211, 221.
144. *See* Carey, *supra* note 132, at 724 (discussing how spousal immunity is applied to intentional torts in some states that retained the doctrine).

violent or threatening acts, harassment, contact, communication, or physical proximity to another person."[145] Depending on the state, the order may be issued under domestic violence laws, family laws, or anti-stalking laws.[146] Provisions in a DVRO can be anything a court finds appropriate that the statute permits: prohibiting contact or abuse, determining child custody and visitation, mandating counseling, prohibiting possession of firearms, and paying support or restitution.[147] DVROs are beneficial because they can deter abuse when a judge enforces compliance through contempt or criminal misdemeanor charges.[148] Unfortunately, in most states, DVROs last for only one year or some other limited duration.[149] Still, they are a commonly sought legal remedy by domestic violence survivors, and can be an important alternative or addition to other remedies.

In the context of tech abuse more broadly, research has shown that survivors are threatened by the inability to obtain and enforce DVROs. For example, while some states consider cyberstalking a felony if a survivor has a protection order against the perpetrator,[150] other states provide no laws requiring courts to issue protection orders based on cyberstalking.[151] Regarding enforcement, it is not always clear what "no contact" means. Studying various cases in Australia, one researcher found that for some violations, it was unclear whether the abusers knew that the DVROs issued against them extended to digital harassment.[152] Other abusers who understood that DVROs covered digital harassment still saw such orders as "merely a piece of paper" and intentionally breached the provisions.[153] IoT-facilitated abuse is even more susceptible to these current limitations. To address these issues, the following changes are critical. First, to ensure that survivors of IoT-facilitated abuse can seek DVROs, legislators should clarify that courts have the authority (1) to issue DVROs based on tech abuse,[154] and (2) to include specific provisions requiring the abuser not to interfere with the survivor's IoT devices and to remove himself from those

145. Stoever, *supra* note 19, at 1019.

146. *Id.* Note that if a victim's state has no specific restraining order for stalking or she does not qualify for a DVRO, she still may be able to get one from a criminal court if the stalker is arrested and charged. *Stalking/Cyberstalking*, *supra* note 22.

147. Shimizu, *supra* note 23, at 121.

148. *Id.*

149. Stoever, *supra* note 19, at 1018.

150. In Ohio and Washington, cyberstalking becomes a felony if the perpetrator is subject to a protection order, and in Washington, the victim does not even have to be the individual protected under the order. *See* OHIO REV. CODE ANN. § 2903.211(B)(2)(g) (West 2020); WASH. REV. CODE ANN. § 9.61.260(3)(a) (2020).

151. *See, e.g.*, MD. CODE ANN., FAM. LAW § 4-506(d) (West 2020) (permitting relief from harassment but not mentioning stalking or cyberstalking at all).

152. Al-Alosi, *supra* note 30, at 1587.

153. *Id.* at 1593.

154. *See, e.g.*, CAL. FAM. CODE §§ 6203, 6320(a) (2020) (establishing that courts may enjoin abusive contact made either directly or indirectly, including—with reference to provisions of the California Penal Code—by electronic means); *id.* § 6203.

accounts. Second, to address the confusion around no-contact provisions, courts should include a definition of "contact" within the order that covers indirect contact through electronic and networked devices. Finally, to deter deliberate violations, courts must enforce compliance through contempt or criminal misdemeanor charges.

3. Federal Civil Remedy

There is no civil cause of action for domestic violence at the federal level.[155] The 1994 Violence Against Women Act (VAWA), enacted under Title IV of the Violent Crime Control and Law Enforcement Act of 1994, created a civil rights remedy allowing survivors of a "crime of violence motivated by gender" to sue for money damages.[156] However, in 2000, the Supreme Court struck down the remedy in *United States v. Morrison* and held that the Commerce Clause did not authorize Congress to enact such a provision.[157] Because there is no federal civil remedy for domestic abuse, survivors and advocates have little choice but to leverage state remedies such as DVROs and tort claims.

The lack of a federal remedy has significant consequences. Given the disparities in state law responses to tech abuse, women in some states will inevitably have less access to remedies compared to women in other states. A federal remedy would preserve or create a minimum civil remedy for women regardless of where they live. And ideally, states would create even broader protections. However, a revival of VAWA's civil remedy would not be effective because the provision's primary intent was merely symbolic.[158] Rather, policy advocates should seek to create a federal statutory remedy under which women can realistically litigate and redress their harm.

Practically, however, attempts to create a federal civil remedy will likely face an uncompromising federalism challenge by states, under *Morrison*'s ruling that domestic violence does not substantially affect interstate commerce.[159] Thus, instead of fighting for a federal remedy, expanding the availability of state tort claims and DVROs for IoT-facilitated abuse may be the most effective and efficient means of bringing about reform.

---

155. Shimizu, *supra* note 23, at 127–28.

156. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 40302(c), 108 Stat. 1796, 1941 (codified at 34 U.S.C. § 12361(c)), *declared unconstitutional by* United States v. Morrison, 529 U.S. 598 (2000).

157. 529 U.S. 598, 618 (2000) (holding that gender-motivated crimes of violence were not an economic activity and did not substantially affect interstate commerce).

158. Caroline S. Schmidt, Note, *What Killed the Violence Against Women Act's Civil Rights Remedy Before the Supreme Court Did?*, 101 VA. L. REV. 501, 524–26 (2015) (quoting statements from National Organization of Women leader Sally Goldfarb and from then-Senator Joseph R. Biden at a 1990 congressional hearing, and demonstrating that the primary purpose of the civil cause of action was to declare that the government considered violence against women a crime).

159. Shimizu, *supra* note 23, at 128.

C. Criminal Remedies

Criminal remedies differ from civil remedies because they emphasize the perpetrator's wrongdoing rather than the survivor's harm. Some legal scholars argue that criminal remedies are important for this reason. Criminal remedies enlist the force of the state to punish the perpetrator rather than simply compensate the survivor. In addition, criminal remedies may be more effective at conveying social condemnation compared to civil remedies.[160]

Notwithstanding the power of criminal remedies to punish the perpetrator and incapacitate them via imprisonment, carceral solutions to domestic violence can be problematic. In 2000, Angela Davis noted that the legal conception of violence against women as a crime had not decreased domestic violence, but instead contributed to "sequestering" millions of men in America's expanding prison system.[161] She urged her audience to consider the following: "Does giving women greater access to official [state] violence help to minimize informal [interpersonal] violence?"[162] Relatedly, in their 2001 *Statement on Gender Violence & the Prison Industrial Complex*, organizers from Incite! Women of Color Against Violence[163] and Critical Resistance shed light on how the anti-domestic violence movement and the anti-prison movement created contradictory visions of safety, collaborating with law enforcement on one hand and resisting prisons and policing on the other.[164] Seven years later, Incite! and Critical Resistance renewed their call for social justice movements to develop strategies that address "both state and interpersonal violence" so that survivors can live violence-free lives without relying on the criminal justice system.[165]

Many domestic violence service providers and survivors share this hesitation to engage with the criminal justice system. In 2015, a group of researchers from CUNY School of Law, University of Miami School of Law, and the American Civil Liberties Union (ACLU) conducted a field study regarding policing and domestic violence.[166] The study analyzed more than nine-hundred survey responses nationwide.[167] The authors found a wide range of concerns, and sorted them into the following four categories of concerns: (1) police inaction, hostility, or dismissiveness toward survivors; (2) police bias

160. Al-Alosi, *supra* note 30, at 1603.

161. Angela Davis, *The Color of Violence Against Women*, COLORLINES (Oct. 10, 2000), https://www.colorlines.com/articles/color-violence-against-women [https://perma.cc/77EU-NASP].

162. *Id.*

163. Now known as INCITE! Women, Gender Non-Conforming, and Trans People of Color Against Violence.

164. CR10 PUBL'NS COLLECTIVE, ABOLITION NOW! 15–16, 21 (2008) (reproducing a 2001 statement).

165. *Id.* at 15, 21.

166. JULIE GOLDSCHEID ET AL., CUNY SCH. OF L. ET AL., RESPONSES FROM THE FIELD: SEXUAL ASSAULT, DOMESTIC VIOLENCE, AND POLICING (2015), https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1075&context=cl_pubs [https://perma.cc/Q4BM-U23D].

167. *Id.* at 1.

against survivors due to their gender, race, immigration status, socioeconomic status, sexual orientation, gender identity, or other identity; (3) the collateral consequences of law enforcement involvement, including involvement by child protective services, immigration enforcement, and retribution from the abuser; and (4) the criminal justice system's focus on punishment rather than the survivors' goals of separation or healing.[168] The themes in these concerns appear to be a fear that the police will not believe the survivor and that calling the police will widen the carceral net, either by implicating the survivor in a crime or implicating her abuser and community members. Especially in communities of color where police are not seen as protectors, a woman who calls the police and invites them into the community may not only risk harm to community members but also jeopardize any support she may have received from them.

This Note embraces the view that survivors of domestic violence must be empowered to utilize whichever solutions they believe will mitigate or eliminate their individual experiences of abuse. As a result, the remainder of this Section describes and analyzes existing criminal laws that may be applied in cases of IoT-facilitated abuse. Recognizing these valid critiques of carceral solutions, however, the Note will discuss nonlegal remedies in Part III.D that address IoT-facilitated abuse without relying on the criminal or civil legal systems.

1. Stalking and Cyberstalking Laws

Stalking laws may provide a critical remedy for many survivors of IoT-facilitated abuse. On the federal level, Congress first passed the Interstate Stalking Punishment and Prevention Act—codified at 18 U.S.C. § 2261A—in 1996.[169] Legislators amended the statute in 2013 as part of the reauthorization of VAWA, broadening the requisite mens rea to criminalize the intent to "harass . . . or place under surveillance"; expanding the crime to include causing "substantial emotional distress"; and extending the mechanism of injury to include "any interactive computer service or electronic communication service or electronic communication system of interstate commerce."[170] Even before the 2013 amendment, the Second Circuit held in 2011 that evidence of the defendant tracking the survivor with a GPS device was relevant to the abuser's intent and the survivor's fear.[171] Section 2261A has not been used for IoT-facilitated abuse, but the inclusion of "electronic communication systems" suggests that the statute could apply to stalking committed via networked devices.

168. *Id.* at 1–2. For further discussion of how police officers minimize the experiences of survivors who report abuse, see *supra* Part II.B.

169. National Defense Authorization Act for Fiscal Year 1997, Pub. L. No. 104-201, § 1069(a), 110 Stat. 2422, 2655 (1996) (codified as amended at 18 U.S.C. § 2261A).

170. Violence Against Women Reauthorization Act of 2013, Pub. L. No. 113-4, § 107(b), 127 Stat. 54, 77.

171. United States v. Curley, 639 F.3d 50, 58–59 (2d Cir. 2011).

In addition to the federal stalking statute, stalking is a crime in all fifty states.[172] However, states vary in their responses to addressing cyberstalking: a few states recognize it as a distinct crime;[173] many incorporate elements of cyberstalking within their stalking statutes such that the language can be interpreted to include cyberstalking;[174] and some do not address it at all.[175] Aily Shimizu has argued that a comprehensive criminal stalking statute must include five elements: (1) addressing the use of electronic communications; (2) eliminating the requirement for a physical threat; (3) including anonymous communications; (4) removing the requirement that communication be directed at the survivor; and (5) addressing third-party inducement.[176] She found that only Ohio, Rhode Island, and Washington included all five elements in their state stalking statutes.[177]

Though Shimizu directed her suggestions for change toward cyberstalking laws, they are nonetheless instructive for cases involving IoT-facilitated abuse. First, statutes should not include a physical threat requirement because IoT-facilitated abuse does not require physical harm. Second, statutes should not require that communication be directed at the survivor because stalking someone by using an IoT device is indirect. By not removing this directness requirement for communications, even a statute that covers electronic "communications" would fail to include IoT devices. "Jackie's Law" in New York provides a potential solution. Seeking to address cyberstalking, Jackie's Law amended a section of New York's stalking statute to include GPS tracking within the meaning of "following."[178] Using Jackie's Law as a model, a statute inclusive of IoT-facilitated abuse would state: "'Following' shall include the unauthorized tracking of such person's movements or location through the use of 'smart' or internet-connected devices." State stalking laws should remove any physicality and directness requirements that would disqualify claims of IoT-facilitated abuse, and also explicitly include networked devices as instruments of stalking.

---

172. Baddam, *supra* note 20, at 85.

173. Only Illinois, Louisiana, Michigan, North Carolina, Rhode Island, and Washington had legislation exclusively addressing cyberstalking as of 2007. Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 144 (2007).

174. *See, e.g.*, CONN. GEN. STAT. § 53a-181 (2019) (maintains a physical pursuit requirement and thus fails to address cyberstalking entirely).

175. *See, e.g.*, N.Y. PENAL LAW § 240.30(a) (McKinney 2020) (covers communications by electronic means but does not include indirect threats or threats through third-party inducement).

176. Shimizu, *supra* note 23, at 120.

177. *Id.* at 120–21.

178. *See* Act of July 23, 2014, ch. 184, 2014 N.Y. Laws 922 (codified at N.Y. PENAL LAW § 120.45); Press Release, Timothy M. Kennedy, N.Y. State Senate, Governor Cuomo Signs Jackie's Law, Authored by Senator Kennedy and Assemblywoman Peoples-Stokes, to Crack Down on GPS Stalking and Domestic Violence (July 23, 2014), https://www.nysenate.gov/newsroom/press-releases/timothy-m-kennedy/governor-cuomo-signs-jackies-law-authored-senator-kennedy [https://perma.cc/S5HM-PQGZ].

2. Harassment Laws

If an abuser's actions do not rise to the level of stalking, a survivor might still be able to turn to criminal harassment laws. Michigan's Penal Code is a helpful model. In Michigan, harassment includes "repeated or continuing unconsented contact" that causes "a reasonable individual to suffer emotional distress."[179] The statute's definition of "unconsented contact" includes, but is not limited to, calling someone's telephone and sending them mail or electronic communications.[180] Similar to making phone calls or sending emails, an abuser can misuse IoT devices to harass someone without directly contacting them. It is possible that this law could be applied to survivors of IoT-facilitated abuse because it does not purport to limit the definition of "contact." However, without explicit inclusion of networked devices in those definitions, harassment claims for IoT-facilitated abuse may be vulnerable to attack. For instance, the defendant can claim that he was merely interacting with the device, which is what IoT devices are designed for, rather than using the device as a medium to contact the survivor. Accordingly, anti-harassment statutes in all states should broadly define "contact" to encompass unconsented exposure to remote-controlled monitoring or actions by another user, such as unconsented changing of temperature on a smart thermostat or ringing of doorbells when no one is outside. To address IoT-facilitated abuse, states must strive to pass anti-harassment laws that adequately account for remote contact.

3. Surveillance Laws

Existing laws against surveillance can also provide criminal remedies for survivors of IoT-facilitated abuse. The NNEDV defines electronic surveillance as watching or monitoring a person's actions or conversations using electronic devices or platforms, without the person's knowledge or consent.[181] Cyber-surveillance, which is similar but not exactly identical, occurs when someone uses "smart" or networked devices to monitor another person.[182]

Electronic surveillance laws include laws against eavesdropping and wiretapping, which could be used against an abuser who employs IoT devices to interfere with the survivor's private conversations to listen to or record them. Under federal law, it is a crime for a non-party to intercept a conversation unless at least one party in the exchange knowingly consents.[183] Most state laws are similar to the federal statute, but fifteen states require consent from all parties

179. MICH. COMP. LAWS ANN. § 750.411h(1)(c) (West 2020).

180. *Id.* § 750.411h(1)(e).

181. *Abuse Using Technology*, NAT'L NETWORK TO END DOMESTIC VIOLENCE: WOMENSLAW.ORG, https://www.womenslaw.org/about-abuse/abuse-using-technology/all [https://perma.cc/7W3C-JA6U].

182. *Id.* (stating that electronic surveillance laws "could" apply, or "perhaps" may apply—thus implying that they also may *not* apply).

183. 18 U.S.C. § 2511.

before a conversation may be recorded.[184] Some states require consent only in situations where the party has no objectively "reasonable expectation of privacy."[185] If an abuser uses the audio feature of an IoT device to listen to the survivor's conversations without being a party to that conversation, eavesdropping laws would apply regardless of whether state law required one-party or all-party consent. More importantly, in cases where reasonable expectation of privacy is at issue, courts must hold that the survivor has a reasonable expectation of privacy in her home.

Michigan law provides a useful blueprint for another criminal surveillance law that states should enact to protect survivors of IoT-facilitated abuse. In Michigan, it is a crime to "[i]nstall, place, or use in any private place, without the consent of the person or persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place."[186] Typically, invasion of privacy is a civil tort, but some states such as Michigan have criminal invasion of privacy laws.[187] Michigan is also unique because it criminalizes unlawful invasions via "any device," which is likely broad enough to include IoT devices.

Finally, IoT-facilitated abuse likely falls under surveillance laws if the abuser uses IoT devices with cameras—e.g., security cameras, video doorbells, or smart home systems powered by mounted iPads—to capture intimate images, video, or audio recordings of the survivor. Furthermore, if the captured images or videos are intimate in nature and the abuser then disseminates them without the survivor's knowledge and permission, the conduct constitutes revenge porn and additional laws apply. "Revenge porn" is a frequently used (and somewhat misleading) term that refers to the sharing of explicit or sexual images or videos without the consent of the person in the image.[188]

184. For a fifty-state survey of recording statutes, see JUSTIA, RECORDING CALLS AND CONVERSATIONS (2018), https://www.justia.com/documents/50-state-surveys-recording-calls-and-conversations.pdf [https://perma.cc/LWP9-Z845].

185. *See, e.g.*, Flanagan v. Flanagan, 41 P.3d 575, 576–77 (Cal. 2002) (endorsing the standard that a conversation is confidential if "a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded"); Malpas v. State, 695 A.2d 588, 595 (Md. Ct. Spec. App. 1997) (endorsing a similar standard).

186. MICH. COMP. LAWS § 750.539d(1)(a) (2020).

187. RESTATEMENT (SECOND) OF TORTS §§ 652A–652I (1977) (reciting four categories of protected interests: protection from unreasonable intrusion upon one's seclusion, from appropriation of one's name or likeness, from unreasonable publicity given to one's private life, and from publicity which unreasonably places one in a false light before the public).

188. *Frequently Asked Questions*, CYBER CIV. RTS. INITIATIVE, https://www.cybercivilrights.org/faqs/ [https://perma.cc/VY6Q-NS4V] (explaining that the term is misleading because the focus should be on the distribution of the images rather than the motivation of the abuser for revenge, as many other motives can be at play; in tech abuse, the motive could also be to assert power and control).

Forty-six states, the District of Columbia, and Guam currently have laws against distribution of revenge porn, but they all take different approaches.[189] Some added revenge porn to existing statutes, while others drafted new ones; some classify the offense as a misdemeanor while others consider it a felony.[190] Another inconsistency (and flaw) is that several revenge porn statutes contain an intent requirement.[191] At the time it passed in 2015, Illinois's statute was considered the country's strongest revenge porn legislation because it eliminated the intent requirement.[192] Revenge porn causes harm the moment it is disseminated, and the harm is multiplied each time the image is shared or viewed. This harm to the survivor exists regardless of the perpetrator's motive. Moreover, intent requirements create an additional barrier for survivors in their legal battles. Especially in the age of technological advances and the IoT, a consistent approach is needed: states must eliminate intent requirements from their revenge porn statutes.

D. Non-Legal Remedies

The legal system alone is not sufficient to address domestic violence. For example, a DVRO that requires an abuser to stop contacting the survivor, including via IoT devices, will only prevent the abuse for a limited time. Eventually, the DVRO will expire and the survivor will have to either return to the court system to renew the order or face the abuser's resuming contact. However, relying on the legal system can be re-traumatizing because the survivor must recite the facts of her abuse and prove to the court that she deserves continuing protection.[193] In addition, there are barriers to seeking legal remedies:

189. For a compilation of the relevant criminal code sections in each state and territory, see *46 States + DC + One Territory Now Have Revenge Porn Laws*, CYBER CIV. RTS. INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/ [https://perma.cc/EW9E-F9XG].

190. Jillian Roffer, *Nonconsensual Pornography: An Old Crime Updates Its Software*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 935, 938 (2017). New Jersey is a state that revised its existing statute. *See, e.g.*, N.J. STAT. ANN. § 2C:14-9(c) (West 2020) (including revenge porn law in invasion of privacy statute). States that enacted new statutes include California, Florida, and North Carolina. CAL. PENAL CODE § 647 (West 2020) (California's "disorderly conduct" statute); FLA. STAT. § 784.049 (2020) (Florida's "sexual cyberharassment" statute); N.C. GEN. STAT. § 14-190.5A (2019) (North Carolina's "disclosure of private images" statute). Whereas Louisiana classifies the distribution of revenge porn as a felony, Connecticut treats it as a class A misdemeanor. *Compare* LA. STAT. ANN. § 14:283.2 (West 2020), *with* CONN. GEN. STAT. § 53a-189c (2019).

191. *See, e.g.*, ARIZ. REV. STAT. ANN. § 13-1425 (2020) (requiring intent to harm, harass, intimidate, threaten, or coerce the depicted person); D.C. CODE § 22-3052 (2020) (requiring intent to harm the person depicted or to receive financial gain).

192. 720 ILL. COMP. STAT. ANN. 5/11-23.5 (2020); *see also* Barbara Herman, *Illinois Passes Revenge Porn Law with Teeth: 'Other States Should Copy,' Says Privacy Lawyer*, INT'L BUS. TIMES (Jan. 6, 2015), https://www.ibtimes.com/illinois-passes-revenge-porn-law-teeth-other-states-should-copy-says-privacy-lawyer-1774974 [https://perma.cc/H4EQ-C3CE].

193. For example, in California, courts do not require survivors to prove additional abuse but still require them to explain "why [they] are afraid of abuse in the future." *See* CAL. FAM. CODE § 6345(a) (West 2020); JUD. COUNSEL OF CAL., FORM DV-700: REQUEST TO RENEW RESTRAINING ORDER

the survivor must have the tools to recognize her own situation as abusive—which is not always obvious in contexts of nonphysical abuse—as well as the financial means to obtain legal assistance or representation.

Some authors even argue that the legal system is not the *right* place for women to turn to for help. Leigh Goodmark has explained that current laws improperly demand physical violence before taking abuse seriously, strip survivors of agency due to "mandatory arrest" policies, and deprive them of dignity by doubting their judgment and parenting ability.[194] As discussed in Part III.C, the criminal justice system serves the goals of retribution, but often risks severe punitive consequences for both the survivor and members of her community.[195]

Finally, even where the legal system may be effective, it is only available after the survivor has already been harmed—it does not have the power to preemptively keep survivors safe. With these criticisms in mind, the following Section will explore four non-legal remedies: cultural change, digital safety training, community accountability strategies, and safer design. These remedies differ from the previous remedies discussed in this Note because they do not rely on civil or criminal laws and they have the potential to stop harm before it occurs.

1. Cultural Change

To mitigate IoT-facilitated abuse, the most important starting point is not in the civil, criminal, or family law system, but with cultural change. Cultural change can seem abstract and is admittedly difficult to achieve in the short term. However, cultural attitudes are critical because they affect whether survivors will come forward about their abuse in the first place; whether players in the civil and

(2012), https://www.courts.ca.gov/documents/dv700.pdf [https://perma.cc/RR4P-7T84]. In Oregon, the abuser has the right to request a court hearing to fight a grant of renewal. OR. REV. STAT. § 107.725(4) (2019). In Texas, the renewal filing must describe what the abuser did to place the survivor in "fear of imminent . . . harm." TEX. FAM. CODE ANN. § 82.0085(a)(2) (West 2020).

194. Leigh Goodmark, *Law Is the Answer? Do We Know That for Sure?: Questioning the Efficacy of Legal Interventions for Battered Women*, 23 ST. LOUIS U. PUB. L. REV. 7, 28, 30, 35 (2004). Mandatory arrest policies require police responding to a 911 call to make an arrest when they have probable cause to believe a person committed an act of domestic violence. CTR. FOR RSCH. ON VIOLENCE AGAINST WOMEN, UNIV. OF KY., TOP TEN THINGS ADVOCATES NEED TO KNOW: QUESTION 5: WHAT IS THE IMPACT OF MANDATORY ARREST LAWS ON INTIMATE PARTNER VIOLENCE VICTIMS AND OFFENDERS? 1 (2011), https://opsvaw.as.uky.edu/sites/default/files/05_Mandatory_Arrest.pdf [https://perma.cc/8BBZ-K7BE]. They are *not allowed* to ask the apparent victim whether she wants to press charges or have the apparent perpetrator arrested—this is why advocates argue that the criminal legal system deprives women of agency. *See id.* at 1–3. Some states do not have laws for primary offenders, which leads to high rates of dual arrests when the police cannot discern who the primary offender is. *See* DAVID HIRSCHEL, DOMESTIC VIOLENCE CASES: WHAT RESEARCH SHOWS ABOUT ARREST AND DUAL ARREST RATES tbl.1 (2008), https://www.ncjrs.gov/pdffiles1/nij/222679.pdf [https://perma.cc/Z6FC-RR7X]. A few states have "preferred arrest" policies, under which arrest is still the preferred response, but officers are not obligated to make an arrest. *See id.* tbl.2.

195. *See* Davis, *supra* note 161; CR10 PUBL'NS COLLECTIVE, *supra* note 164; GOLDSCHEID ET AL., *supra* note 166, at 1–2.

criminal legal systems will be willing to apply or expand existing laws to protect those survivors; and whether community members will take the allegations of abuse seriously enough to offer support.

Part II.C described implications of the IoT for domestic violence, including a form of victim-blaming that tells survivors that they are responsible because they failed to stop using their smart devices, and a form of minimization that discounts the psychological trauma caused by nonphysical violence such as IoT-facilitated abuse. To combat victim-blaming and minimization, it is important to expand the social understanding of what domestic violence looks like.

A sign of positive change is that it is no longer radical to view domestic violence as "coercive control." Even the federal government of the United States recognized this definition, at least, prior to the Trump administration's revision.[196] However, the commonly referenced materials in domestic violence work insufficiently address the issue of tech abuse as a tactic of coercive control. For instance, the Power and Control Wheel includes physical, sexual, and emotional abuse, but does not include tech abuse.[197] Although tech abuse is highly linked to other elements on the Wheel such as emotional abuse, intimidation, and isolation, tech abuse should nevertheless be added as a separate spoke with its own description of common and emerging tactics.

Beyond updates to the Wheel, advocates who interact with survivors must be explicit and insistent in stating that tech abuse and IoT-facilitated abuse constitute domestic violence. This will encourage survivors to recognize abusive situations and reduce third-party attempts to minimize the survivor's experiences. First, survivors of nonphysical abuse may not recognize that they are experiencing domestic violence. This is especially true for young people because they tend to accept a certain level of privacy invasion as a tradeoff for their constantly connected lives.[198] However, survivors will be more likely to recognize IoT-facilitated abuse if every domestic violence website has a page about tech abuse, if every domestic violence hotline offers the option to speak about potential tech abuse, and if every shelter conducts risk assessments that include tech abuse. Second, if tech abuse and IoT-facilitated abuse are listed explicitly across a wide range of domestic violence resources, lawyers and other advocates will be better able to argue that the survivor qualifies for remedies under harassment, cyberstalking, or other laws. For instance, domestic violence experts often rely on the Power and Control Wheel when testifying in court; if the Wheel lists IoT-facilitated abuse, an expert will be more likely to educate and convince judges and juries that the defendant's actions constituted domestic violence.

196. *See supra* note 125 and accompanying text.

197. DOMESTIC ABUSE INTERVENTION PROGRAMS, *supra* note 13.

198. *See supra* Part I.B (discussing teens and the challenges posed by their increasing reliance on technology).

Moreover, this cultural change can begin in personal networks. For example, a technology specialist at NNEDV's Safety Net Project (the "Project") suggested a "survivor-driven and empowering" approach to interacting with survivors.[199] Because abusers often gaslight survivors and third parties may have the initial instinct to minimize IoT-facilitated abuse, a survivor-driven approach requires us to intentionally and attentively believe our friends or coworkers when they say they are experiencing abuse.

Technology can be a "powerful weapon of control" for abusive partners, and abusers can "turn someone's technological world against them" through access to the survivor's electronic devices.[200] Changing the cultural understanding of domestic violence to include tech abuse and IoT-facilitated abuse will ensure that survivors, advocates, and actors in the legal system alike recognize these tactics of abuse.

2. Digital Safety Training

Technology can provide benefits to survivors, including communication with friends and family, convenience in daily life, and access to support. Thus, the goal must be to ensure that survivors know how to safely use technology, not to ask them to disconnect from technology. For this reason, digital literacy and safety training can be a critical avenue for preventing or decreasing IoT-facilitated abuse.

The NNEDV created the Project in the late 1990s, which educates survivors, advocates, and other professionals working with survivors on how technology impacts the safety, privacy, accessibility, and civil rights of survivors.[201] The Project continues to create training resources on how technology can be misused, how to strategize for technology safety, how survivors can relocate, how to keep survivor data confidential, and how agencies can safely use technology.[202] It shares these resources and provides interactive trainings to various groups that work with survivors of abuse, including local domestic violence shelters, law enforcement officers, and community legal service providers; the Project also hosts an annual Technology Summit in Silicon Valley.[203] More recently, with the growth of the IoT, the Project has been providing expert technical assistance to survivors who report that "Alexa is turning things on and off" or who are "hearing voices."[204] In March 2019, University College London's Gender and IoT project also compiled a six-page

199. BWJP, *supra* note 31, at 48:40–50:52 (presentation by Rachel Gibson).

200. Elinor Jordan & Sarah Prout Rennie, *Supporting Victims of Technology-Facilitated Abuse*, MICH. BAR J., July 2019, at 34, 34–35.

201. *Technology Safety*, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://nnedv.org/content/technology-safety/ [https://perma.cc/46AZ-PHP3].

202. *Id.*

203. *Id.*

204. BWJP, *supra* note 31, at 31:02–:16 (presentation by Rachel Gibson).

list of such resources.[205] The list includes explanations of how to spot and engage with networked devices; digital security information on cyberstalking and blackmail; guides for securing passwords and social media accounts; and recommendations for the setup, maintenance, and disposal of IoT systems.[206] Following these examples, all groups that work with survivors of domestic violence should make resources for tech safety available online and in person. However, digital safety will not fully serve deterrence goals if it is shared solely with survivors who seek help for abuse that has occurred or is ongoing. Rather, information regarding abusive behavior perpetrated via technology and guidelines for IoT safety should be distributed broadly. For instance, digital safety trainings should be incorporated into internet safety lessons that parents and teachers share with teens.

Finally, the Family Justice Center may be an additional location for digital safety training. Currently, Family Justice Centers across the country co-locate multiple organizations as a "one stop shop" providing services to survivors of interpersonal violence including intimate partner violence, sexual assault, child abuse, elder or dependent adult abuse, and human trafficking.[207] A center typically has law enforcement personnel, domestic violence shelter staff, civil legal service providers, housing services staff, social service agency staff, county health department staff, employment counselors, and other agencies' personnel.[208] There is a strong critique of this model: opponents warn that, with multiple groups that serve different goals located together, domestic violence workers' anti-violence and empowerment missions can be negatively influenced by criminal justice and governmental involvement.[209]

However, advocates could reimagine a Family Justice Center model that opposes both interpersonal violence and state violence—one that continues to partner with agencies such as community advocates, shelters, and employment services, but excludes law enforcement personnel. In designing what I will call a "violence-free Family Justice Center," advocates should collaborate with privacy and technology specialists such as the advocates from the Project. For example, a new technology-clinic model is currently operating in New York City

205. LEONIE TANCZER, ISABEL LOPEZ-NEIRA, TRUPTI PATEL, SIMON PARKIN, &GEORGE DANEZIS, UNIV. COLLEGE LONDON, GENDER AND IOT (G-IOT) RESOURCE LIST (2019), https://www.ucl.ac.uk/steapp/sites/steapp/files/g-iot-resource-list.pdf [https://perma.cc/VHF2-GWMD].

206. *Id*.

207. *See Jane K. Stoever, Mirandizing Family Justice*, 39 HARV. J.L. & GENDER 189, 200 (2016); About Family Justice Centers, FAM. JUST. CTR. ALL., https://www.familyjusticecenter.org/affiliated-centers/family-justice-centers-2/ [https://perma.cc/P77A-W5VE] (last visited July 22, 2020).

208. Stoever, *supra* note 207, at 201.

209. *Id*. at 203.

Family Justice Centers.[210] The model was developed in 2019 by Cornell Tech researchers working in conjunction with the New York City Mayor's Office to End Domestic and Gender-Based Violence, and it includes a technology assessment questionnaire, a spyware scanning tool that is undetectable by abusers, and a diagram that summarizes a survivor's digital footprint.[211] Other services might include risk assessments for tech abuse and providing personalized strategies for safety. Most importantly, however, the violence-free Family Justice Center must ensure that tech abuse specialists have both the technical skills to detect and mitigate a client's digital vulnerabilities, and the training in trauma-informed and survivor-centered approaches in order to offer solutions that will not inadvertently endanger the survivor.

3. Community Accountability and Transformative Justice

As mentioned in Part II.C, many police departments are currently ill-equipped to investigate tech abuse. The seemingly straightforward solution would be to increase funding for law enforcement so they can properly handle cybercrimes. However, there is growing evidence that police officers have not succeeded in stopping domestic violence. In fact, they have contributed greatly to it.

In *Police Wife: The Secret Epidemic of Police Domestic Violence*, the author notes that 40 percent of U.S. police officers admitted to being violent with their spouse or children.[212] The author also described a "blue wall of silence": an unwritten understanding among fellow officers that they will protect each other from investigation for misconduct as a "professional courtesy."[213] Unsurprisingly, a 2013 *New York Times* investigation of Florida Police Departments found that "nearly 30 percent of the officers accused of domestic violence were still working in the same agency a year later, compared with 1 percent of those who failed drug tests and 7 percent of those accused of theft."[214] There is even a specific Power and Control Wheel for "Police Perpetrated Domestic Violence," which includes unique tactics such as knowledge of the law and the court system, possession of weapons and training in use of force, and

210. Melanie Lefkowitz, *New Tools Help Detect Digital Domestic Abuse*, CORNELL CHRON. (Aug. 13, 2019), https://news.cornell.edu/stories/2019/08/new-tools-help-detect-digital-domestic-abuse [https://perma.cc/XB2W-A6NU].

211. *Id.*

212. ALEX ROSLIN, POLICE WIFE: THE SECRET EPIDEMIC OF POLICE DOMESTIC VIOLENCE 6–7 (2015).

213. *Id.* at 92.

214. Sarah Cohen, Rebecca R. Ruiz & Sarah Childress, *Departments Are Slow to Police Their Own Abusers*, N.Y. TIMES (Nov. 23, 2013), http://www.nytimes.com/projects/2013/police-domestic-abuse/index.html [https://perma.cc/EL3U-49NY]. The authors investigated Florida because the state has one of the most robust open records laws in the United States. *Id.*

high status in the community.[215] These facts generate doubts regarding the mainstream anti-domestic violence movement's reliance on the criminal justice system. If survivors are supposed to call the police to stop domestic violence, where do the women who suffer from police-perpetrated domestic violence turn? Also, how can survivors trust police officers to respond to domestic violence if they know that many officers are themselves abusers?

Given these statistics, it is critical to find alternatives. In fact, advocates and organizers have been working for decades to imagine ways that community resources can be shifted away from policing and imprisonment toward community efforts to mitigate domestic violence. The concepts of transformative justice and community accountability are critical to these efforts. Transformative justice is an approach to harm that seeks safety and accountability within and by communities.[216] It gives support and healing for individual incidents of abuse while aiming to transform the conditions and social forces that allow such harms to occur.[217] Theorized by Incite!, community accountability is also a community-based strategy to address harm without dependence on police and prisons.[218] Generally, it is a process in which a community, e.g., friends, family, church members, and coworkers, work together to (1) create and affirm values that resist abuse and encourage safety; (2) provide safety and support to community members in a way that respects their self-determination; (3) develop strategies to address community members' abusive behavior, including a process for them to take responsibility for and transform their behavior; and (4) transform the political conditions that reinforce violence.[219] These strategies can repair harm and potentially keep a relationship intact. Moreover, compared to criminal remedies, which are arguably effective in conveying condemnation from general society,[220] community accountability conveys condemnation from community members that the perpetrator knows and likely feels accountable to.

Numerous organizations have applied community-based models to their work. For example, two advocates created a Community Accountability for Survivors of Sexual Violence Toolkit in 2014 as part of the Shifting From

215. NAT'L CTR. ON DOMESTIC & SEXUAL VIOLENCE, POWER AND CONTROL: POLICE PERPETRATED DOMESTIC VIOLENCE (2004), http://www.ncdsv.org/images/Police-perpetrateddomviolNOSHADING.pdf [https://perma.cc/H9CN-9TY8].

216. CREATIVE INTERVENTIONS, CREATIVE INTERVENTIONS TOOLKIT: A PRACTICAL GUIDE TO STOP INTERPERSONAL VIOLENCE S5–S6 (2020), https://www.creative-interventions.org/wp-content/uploads/2020/08/CI-Toolkit-Final-ENTIRE-Aug-2020.pdf [https://perma.cc/T6BR-PJS6].

217. GENERATIONFIVE, TOWARD TRANSFORMATIVE JUSTICE: A LIBERATORY APPROACH TO CHILD SEXUAL ABUSE AND OTHER FORMS OF INTIMATE AND COMMUNITY VIOLENCE 5 (2007), http://www.generationfive.org/wp-content/uploads/2013/07/G5_Toward_Transformative_Justice-Document.pdf [https://perma.cc/Z8AE-PR9S].

218. INCITE! WOMEN, GENDER NON-CONFORMING, AND TRANS PEOPLE OF COLOR AGAINST VIOLENCE, ORGANIZING FOR COMMUNITY ACCOUNTABILITY (2012), http://www.usprisonculture.com/blog/wp-content/uploads/2012/03/commaccountabilityincite.pdf [https://perma.cc/R6KT-6RYH].

219. *Id.*

220. *See* Al-Alosi, *supra* note 30, at 1603.

Carceral to Transformative Justice Feminisms Conference at DePaul University; they also facilitated a workshop on the same topic at the National Sexual Assault Conference in 2012.[221] Creative Interventions, a resource center committed to community-based interventions, runs a Community-Based Interventions Project that creates flexible and practical community solutions to interpersonal violence (including in a 578-page toolkit).[222] It also runs a StoryTelling & Organizing Project that collects and shares first-person stories from people who successfully ended violence through community-based alternatives.[223]

These community-based responses can likely incorporate interventions for IoT-facilitated abuse. For example, the Creative Interventions toolkit suggests being openminded regarding potential allies and what roles those allies could play;[224] in the case of IoT-facilitated abuse, the responding team could include a community member with a job in IT who can check for hacker activity on the survivor's device,[225] plus a domestic violence advocate who specializes in tech safety and can commit to a long-term role in educating the community about privacy and digital safety. The Creative Interventions toolkit also outlines the steps for perpetrator accountability, which includes recognizing the violence and its consequences in an "accountability letter";[226] in the case of IoT-facilitated abuse, where minimization is likely, this may manifest as the following admission: "Yes, it's true. I changed the lock code to intimidate you, and I recognize that I caused you fear. My instinct to control the lock stemmed from my own insecurity about your leaving the house to spend time with other people. I did not know at the time that this was a tactic of domestic abuse, but now I do. I commit to attending therapy to address my own insecurities and hope that we can continue our relationship. I am deeply sorry."

Giving more money to police departments in hopes that they investigate cybercrimes and tech abuse necessarily involves funding the broader prison industrial complex, which already receives more than eighty billion dollars annually.[227] This money is better utilized to support community-based

221. JANE HERETH & CHEZ RUMPF, COMMUNITY ACCOUNTABILITY FOR SURVIVORS OF SEXUAL VIOLENCE TOOLKIT 1 (2014), https://carceralfeminism.files.wordpress.com/2014/04/cassv-reading-group-toolkit_shifting-from-carceral-to-tj-feminisms_final.pdf [https://perma.cc/DA4P-4J63].

222. *See* CREATIVE INTERVENTIONS, *supra* note 216.

223. *Organizing Resources for StoryTelling and Interventions*, CREATIVE INTERVENTIONS, http://www.stopviolenceeveryday.org/creative-interventions/ [https://perma.cc/Z2TX-XN25].

224. CREATIVE INTERVENTIONS, *supra* note 216, section 4C, at 4, 19.

225. Indeed, there is a reported instance where a victim of tech abuse repeatedly took her smartphone to the police to scan it for spyware and was told that nothing was there, then later took it to her employer's IT department and discovered spyware. Phoebe Braithwaite, *Smart Home Tech Is Being Turned into a Tool for Domestic Abuse*, WIRED (July 22, 2018), https://www.wired.co.uk/article/internet-of-things-smart-home-domestic-abuse [https://perma.cc/69JS-TRKH]. This illustrates that a specialist in a victim's community can be more equipped to respond to abuse.

226. CREATIVE INTERVENTIONS, *supra* note 216, section 4F, at 55–57.

227. *Incarceration*, SENT'G PROJECT, https://www.sentencingproject.org/issues/incarceration/ [https://perma.cc/9GPU-5934] (click + sign at bottom of main "ISSUES" box).

alternatives, including funding more workshops on community-based justice for neighborhoods, employers, and churches; paying activists and organizers to conduct more trainings; subsidizing research to study the results of community-based approaches; and printing and distributing community intervention toolkits to domestic violence shelters and support groups across the United States.

4. Collaborations for Safer Design

In order to address the intersection between technology and domestic violence, it is also important to look beyond the traditional sphere of domestic violence work. Specifically, designers of IoT devices and platforms must collaborate with (or at the very least, consult) advocates working against domestic violence.

The NNEDV already works with companies such as Facebook, Twitter, and Google to improve built-in privacy protections.[228] For example, the NNEDV launched *Privacy & Safety on Facebook: A Guide for Survivors of Abuse* in collaboration with Facebook in 2013.[229] Creators of IoT devices should model this approach. IoT companies can begin by taking suggestions from journalists who focus on issues of tech. For example, one author suggested that IoT devices should be engineered to implement privacy by design, including by supporting multi-user accounts, ensuring that default settings cannot be manipulated, and preventing data-sharing between different users without notice or authorization.[230] Safe design should also include automatic generation of weekly or monthly reports informing users about their data and account logins, a system notification that shows which registered user initiated the controls, and the standard of requiring that users opt into rather than out of data-sharing between members of a household. As another author asserted: "[D]esigners and developers of [IoT] products have a responsibility to fully understand how they impact the lived experiences of women facing domestic abuse. Otherwise, they risk unwittingly assisting perpetrators."[231] This author suggested a "feminist approach" to product design, which might include employing survivors of abuse to test products and make UX recommendations, listening to survivors' lived experiences, and understanding the risks of a shared device ecosystem that is not transparent about which users have access.[232]

228. BWJP, *supra* note 31, at 31:17–32:18 (presentation by Rachel Gibson).

229. Al-Alosi, *supra* note 30, at 1602. The most recent version of the guide, from 2019, is available at https://nnedv.org/wp-content/uploads/2019/07/Library_TH_2018_Privacy_Safety_Facebook_Guide_Survivors_Abuse.pdf [https://perma.cc/S6QU-5PQC].

230. Braithwaite, *supra* note 225.

231. Webb, *supra* note 124.

232. *Id*. UX stands for "user experience," and refers to the process of designing products that provide "meaningful and relevant experiences to users," including via branding, design, usability, and function. *User Experience (UX) Design*, INTERACTION DESIGN FOUND., https://www.interaction-design.org/literature/topics/ux-design [https://perma.cc/6G4T-ZC64].

Companies that make IoT devices clearly presuppose that users in a household trust each other not to misuse the device's smart features as a tool of domestic violence. So that they do not become accomplices to abusers, designers of IoT devices must consider the implications of their products on survivors, collaborate with anti-violence advocates to improve protections, and create user guides that address the risks of shared device ecosystems.

CONCLUSION

Tactics of domestic violence are nothing new. Staff at the Domestic Abuse Intervention Project began documenting common abusive behaviors in 1984,[233] and the concept of coercive control emerged almost fifteen years ago to explain domestic violence as a pattern of behaviors.[234] However, the increasing prevalence of IoT devices has given abusers a powerful new tool to both expand and magnify the traditional harms of domestic violence. As Erica Olsen, the director of the Project, stated, "The behavior is not new, but the technology is."[235]

There are three significant barriers to survivor safety in cases of IoT-facilitated abuse. The first is the rigid societal belief that nonphysical abuse is not true harm. This prevents survivors from seeking help for fear that society will not believe them and affects the willingness of actors in the legal system to act for the survivor's benefit. The second is the legal system's consistent lag behind technological innovation. This manifests not only in the total lack of recognition of IoT-facilitated abuse in current laws, but also in the outdated requirements for direct contact or physical surveillance that actively preempt legal claims based on IoT-facilitated abuse. The third barrier is society's unawareness of the paradox of relying on state violence via the criminal justice system to prevent interpersonal violence. This has resulted in increasing numbers of criminal statutes and harsher arrest policies but has failed to address the root causes of domestic violence and lost sight of the most important goal: preventing domestic violence *before* it occurs.

By surveying potential remedies within and beyond the legal system, this Note sheds light on potential ways for society and the legal system to better protect survivors of IoT-facilitated abuse and hold their perpetrators accountable.

233. *FAQs about the Wheels*, DOMESTIC ABUSE INTERVENTION PROGRAMS, https://www.theduluthmodel.org/wheels/faqs-about-the-wheels/ [https://perma.cc/ZXX9-P2UD].

234. *See* STARK, *supra* note 12.

235. Thebault, *supra* note 39.