A HAUNTED (SMART) HOUSE: SMART HOME DEVICES AS TOOLS OF HARASSMENT AND ABUSE

Dana Holmstrand*

CITE AS: 6 GEO. L. TECH. REV. __ (2022)

TABLE OF CONTENTS

INTRODUCTION

The doorbell rings, but no one is there. The temperature in the home goes from extremely cold to extremely hot without anyone touching the thermostat. Locks change when no one is home or unlock without warning in

* Georgetown University Law Center, J.D. 2021; College of William & Mary, B.A. Public Policy 2015. Many, many thanks to Julie Cohen, Alvaro Bedoya, Amanda Levendowski, and Dan Bateyko for their willingness to engage and incredibly thoughtful comments on this piece. Thank you also to the staff of the Georgetown Technology Law Review for their time and effort to bring this piece to print.

the middle of the night. The refrigerator is mysteriously turned off, leaving all the food inside to spoil. Lights flicker on and off while music blares and people try to sleep. While these vignettes may seem like scenes from a horror movie, they are the lived experiences of survivors of Smart HOme facilitated Tech-abuse (SHOT).[1]

Abusers have repurposed smart home devices, including thermostats, locks, lights, speakers, and doorbells, as weapons of surveillance and control. In many instances, only one person is installing and managing all smart devices in the home. This person has enormous power as the main user on the account with access to all passwords for every device. Even after the abusive partner has left the house, they can turn this power on their former partner if they still have access as a user on the home's smart devices. Abusers can access these systems to turn off lights, unlock doors, and change the temperature at the expense of those still living in the home. Not only are these displays of power inconvenient to the survivor, but they can also be psychologically traumatizing, especially when the survivor does not realize their former partner can access and control the devices in the aforementioned ways.

Victims of intimate partner violence and their supporters are struggling to respond to these threats. Restraining orders, which courts issue to deter harassment, may restrict physical contact or communication with the survivor but do not always contain language restricting an abuser's access to systems within the home. This problem is further exacerbated when a survivor is not aware of all the systems in the home. SHOT will only become more prevalent. In 2017, an estimated 29 million homes in the United States had some kind of connected device, and the number of connected devices is only growing.[2]

This Note aims to shed light on the unique challenges presented by the intersection of abuse and smart home technology.[3] Part I will explore smart home technologies and how they can be used as tools of intimate partner violence and harassment by drawing on survivor and advocate stories.[4] Part II

---

[1] I will be using SHOT throughout this paper to refer to any abusive actions using smart home devices. I take this term from the paper "Are Smart Home Devices Abandoning IPV Victims." Ahmed Alshehri et al., *Are Smart Home Devices Abandoning IPV Victims*, ARXIV, Aug. 15, 2020, 1, 2. In that paper, Alshehri and other scholars provide an analytical framework to distinguish SHOT from other types of tech facilitated abuse. *Id.* at 2.

[2] STATISTA, *Smart Homes in the United States*, 12 (2020).

[3] This paper is primarily focused on smart devices that do not record video or sound (ex. security cameras, Ring doorbells, etc.) in order to focus on the unique challenges devices we would not traditionally consider surveillance tools present.

[4] I will also follow the University of Toronto's Citizen Lab's interchangeable use of victim and survivor to acknowledge the real human impacts of those affected while also honoring "the productive force of survival and community in the face of systemic oppression."

will investigate SHOT's impact on survivors by explaining how explicit information collection clarifies SHOT as a form of surveillance and drawing on parallels in prison and torture literature. Part III will review existing federal and state laws to explain why it is so difficult to prosecute and litigate against abusers and will explain why platform self-regulation is not an appropriate solution. Part IV will offer suggestions for a comprehensive response to SHOT. Without legislative changes, abusers will continue to haunt the homes of their former partners consequence-free.

I. WEAPONIZATION OF SMART HOME TECHNOLOGY

Smart home technologies may appear innocuous—even helpful. They conjure images of the retro-future science fiction promised us: speakers that answer our every question, lights that mirror the routines of our lives, thermostats that save us energy and money, locks that are as easy to open as entering a PIN. People willingly bring these devices into our homes and that may be what makes them so dangerous. Perpetrators of intimate partner violence capitalize on this trust to control current and former partners even from a distance.

In June 2018, the New York Times reported on a trend in intimate partner violence that perplexed advocates and frightened survivors.[5] Perpetrators of intimate partner violence were increasingly using WiFi-enabled appliances, i.e. "smart devices," to remotely control and surveil their partners.[6] Other news outlets in the tech space quickly picked up the story,[7] which even garnered the attention of Senator Amy Klobuchar, who issued a public letter to the Departments of Justice (DOJ) and Health and Human Services calling for additional information and resources "to address and prevent domestic abuse, no matter what form it takes."[8] There has been no action or attention on this issue since.

Christopher Parsons et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry*, 25 (2019).

[5] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. TIMES (June 23, 2018), https://perma.cc/7564-CZT6.

[6] *Id.*

[7] Shawn Knight, *Domestic Abusers are Using Smart Home Gadgets to Exert Control Over Victims*, TECHSPOT (June 26, 2018), https://perma.cc/FWV7-8VEV; Jon Fingas, *Domestic Abusers are Exploiting Smart Home Devices*, ENGADGET (June 24, 2018), https://perma.cc/WA5V-QU6X; *Not Hackers but Exes are Remotely Controlling Smart Devices for Domestic Abuse*, AATSG (June 24, 2018), https://perma.cc/4Y9G-GFRQ.

[8] Press Release, *Klobuchar Urges Departments of Justice, Health and Human Services to Support Victims of Domestic Abuse in the Digital Age,* OFF. OF SENATOR AMY KLOBUCHAR (July 27, 2018), https://perma.cc/7CYT-CBDP.

A. Smart Home Technology Prevalence

Americans have embraced the connected home. As of November 2020, almost 43 million homes in the United States had at least one smart device, or almost thirty-seven percent of all American homes.[9] In most instances, the household has more than one smart device in the home. While smart lights have generally only achieved a twelve percent market penetration rate generally,[10] they have achieved a twenty-one percent market penetration rate among households with a smart speaker.[11]

Smart device adoption is not slowing down. From 2018 to 2019 alone, the number of American homes with at least one smart device rose from thirty percent to thirty-three percent.[12] Smart home households are predicted to reach 70.6 million by 2023, which is nearly double the 34.8 million households in 2018.[13] The relative inexpensiveness of many smart devices, including speakers bolsters this trend.[14] Additionally, companies, like Arcadia Power[15] and Walmart,[16] have offered a smart speaker as a free add-on to an existing service or as part of another package deal further driving smart device adoption.

Unlike their analog predecessors, smart devices are often designed to be controlled remotely. As of 2019, sixty-six percent of those with a smart device cited using an app that controls a single type of product as the primary method of controlling the device.[17] More than thirty-four percent cite a single app that controls different types of smart products as the primary method.[18] Lastly, just over thirty-two percent cite physical controls on the device as the primary method of controlling the device.[19] These statistics suggest whoever has access to the many passwords and apps controlling these devices exercises enormous control over those in the household.

B. From Smart Home Use to Smart Home Abuse

---

[9] STATISTA, *supra* note 2, at 12.
[10] *Id.* at 34.
[11] *Id.* at 35.
[12] *Id.* at 12.
[13] *Id.* at 11.
[14] Bowles, *supra* note 5.
[15] If You Live in Massachusetts, Here's an Easy Way to Get a Free Google Home, THE PENNY HOARDER (Jan. 27, 2020), https://perma.cc/9Z8Y-WZSP.
[16] Dave Johnson, *Get a Google Home Mini with a Disney Frozen II book for $20*, CNET (Dec. 4, 2019), https://perma.cc/TH53-Q6K3.
[17] STATISTA, *supra* note 2, at 42.
[18] *Id.*
[19] *Id.*

Litigation involving smart home device abuse first became prevalent in 2017, according to advocates working in the domestic violence space.[20] Around the same time, domestic violence help lines began receiving calls about "crazy-making" things survivors experienced like smart speakers blasting music out of nowhere and thermostats shifting suddenly to 100 degrees.[21] Graciela Rodriguez, who runs an emergency shelter in San Rafael, California, stated people felt they were losing control of their homes and did not realize this was a form of domestic abuse until being at the shelter for several days.[22]

Potential perpetrators of intimate partner violence have a menu of devices to choose from in order to intimidate and harass. The Safety Net Project at the National Network to End Domestic Violence (NNEDV) offers a non-exhaustive list of smart devices that can be used against survivors: speakers, kitchen appliances, TVs, doorbells, thermostats, lights, cameras, wearables, security systems, children's toys, and locks.[23] An abuser could start playing loud music in the middle of the night to wake a survivor or speak to them through the speaker, all through an app. An abuser could turn off a refrigerator when they know a survivor is out, spoiling all the food inside, and leaving the survivor to wonder whether they turned off the refrigerator by mistake. An abuser could ring a doorbell over and over when no one is there to drive the survivor from the home. An abuser could turn on lights at all hours or flick them on and off to produce a strobe effect.

When taken out of context or in the presence of third parties, an abuser's threats to deploy smart home devices against the survivor may not be interpreted as malicious.[24] For example, one woman's husband had installed security cameras in their home and would text her when he was out of the house to ask what she was watching on television, implying he was watching her from the cameras.[25] This behavior appears innocuous, even caring, but becomes meaningful when understood as a product of abuse.[26] Another woman, who was in the process of leaving her husband, explained her husband "controls the thermostat. He controls the lights. He controls the music."[27] The

[20] Bowles, *supra* note 5.
[21] *Id.*
[22] *Id.*
[23] *Evidence Collection Series: Internet of Things (IoT)*, NATIONAL NETWORK TO END DOMESTIC VIOLENCE, https://perma.cc/DVR5-7WEQ (last visited Nov. 16, 2020).
[24] Elizabeth Yardley, *Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework*, VIOLENCE AGAINST WOMEN 1479, 1481 (2020).
[25] *Id.* at 1483.
[26] *Id.* at 1484.
[27] Bowles, *supra* note 5.

particularized nature of smart devices facilitates personalized abuse that the abuser tailors to specific victim vulnerabilities.[28]

Smart home technologies do not disappear when an abuser leaves the home, temporarily or permanently. In many instances, the devices stay behind and can be used to intimidate and confuse the survivor. Abusers can use smartphone applications to remotely control different devices even while no longer living in the home. For certain smart home technologies, the abuser can simply purchase the device, set it up in the home and, as the authenticated account holder, have the highest permissions available to allow them to control the device and monitor its use.[29] One survivor spoke about how the numbers for the digital lock on her front door would change each day for seemingly no reason after her abuser was no longer living in the home.[30]

The solution is not as simple as turning off the device. Although some devices can be turned off through hard resets or changing the home's WiFi password, there is not a fix that works across all devices. Turning off or disconnecting the devices can trigger escalated violence.[31] Unfortunately, the reality is survivors may often not know how to address specific issues with the device. Eva Galperin, director of cybersecurity at the Electronic Frontier Foundation, notes survivors are "not sure how their abuser is getting in, and they're not necessarily able to figure it out because they don't know how the systems work."[32] Galperin explains survivors instead turn off all devices in the home, which can further isolate the survivor. Much of domestic violence involves isolating the survivor from the outside. In this way, in attempting to escape their abuser, victims are incidentally subjected to further abuse.

II. IMPACTS OF SMART HOME DEVICE ABUSE

At its core, domestic violence is about establishing and maintaining an asymmetric power relationship to control the other party.[33] Often, this can be done through gaslighting,[34] which is shown in stark relief in the smart device context. NNEDV defines gaslighting as a form of emotional abuse used to confuse and shift blame onto the victim that can cause the victim to doubt their

---

[28] Yardley, *supra* note 24, at 1484.

[29] Stewart Mitchell, *How Tech Traps Domestic Abuse Victims*, IT PRO, https://perma.cc/Q5C9-ACTU (Aug. 13, 2020).

[30] Bowles, *supra* note 5.

[31] This can include physical violence; a survivor's risk of being killed by her former intimate partner greatly increases when they have just left the abuser. U.S. BUREAU OF JUST. STAT., VIOLENCE AGAINST WOMEN: ESTIMATES FROM THE REDESIGNED SURVEY 1 (Jan. 2000).

[32] Bowles, *supra* note 5.

[33] *Frequently Asked Questions About Domestic Violence*, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://perma.cc/E4NS-HBRP (last visited Nov. 16, 2020).

[34] *Id.*

sanity and convince them they are responsible for, and therefore able to stop, the abuse.[35] Ruth Patrick, an advocate for domestic abuse survivors in Silicon Valley, described how some of her clients had been placed on psychiatric holds following smart home device abuse.[36] As she explained, "If you tell the wrong person your husband knows your every move, and he knows what you've said in your bedroom, you can start to look crazy. It's so much easier to believe someone's crazy than to believe all these things are happening."[37]

A. Overt Omnipresence

SHOT should be considered a form of surveillance and most closely aligns with the concept of "overt omnipresence." Elizabeth Yardley's model of technology-facilitated abuse categorizes overt omnipresence as "undisguised monitoring and control." [38] Yardley describes how the androcentricity of Western family life permits one party in the relationship to get privileged, primary access to electronic accounts in order to establish omnipresence, i.e. control and view of all aspects of a survivors' life.[39] Smart devices exemplify overt omnipresence because the abuser does not seek to hide they are watching, but rather capitalizes on the survivor knowing they are watching to exert control. Smart speakers, smart locks, and smart thermostats are obvious additions to the home as their installation is difficult to hide.[40] Smart device manipulation's effects are also obvious through control of volume, temperature, and illumination. In order to achieve their abusive ends, abusers rely on victims being aware that such changes are occurring and that such changes are beyond their own control.

Daniel Solove's metaphor of Kafka's *The Trial* additionally clarifies SHOT as surveillance.[41] Solove argues *1984*'s Big Brother has outgrown its usefulness as a metaphor for modern surveillance because the Big Brother metaphor relies on the idea that surveillance uncovers one's hidden world and discloses concealed information. [42] The harm caused by Big Brother is inhibition, self-censorship, and reputational damage.[43] *The Trial* metaphor instead conceptualizes surveillance as an individual's lack of control over the

---

[35] *Id.*
[36] Bowles, *supra* note 5.
[37] *Id.*
[38] Yardley, *supra* note 24, at *3.
[39] *Id.*
[40] You could disguise a lightbulb, I suppose.
[41] Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1398 (July 2001).
[42] *Id.* at 1415–16.
[43] *Id.* at 1417.

data collected on them and how it is used by a nameless, faceless authority.[44] Joseph K., *The Trial*'s protagonist, seeks relief from a judicial system that seems to have a vast dossier on him when he has no information on them.[45] Solove theorizes this power and information imbalance is what makes *The Trial* an effective metaphor for modern day surveillance.[46] Databases and associated practices disempower and dehumanize people by stripping them of control over personal information collection and use.[47]

A similar disempowerment is at work in SHOT. Abusers collect information on their victims and exercise control by impacting the environment around the victim. Victims, who often lack access to the passwords and other device controls, cannot affect the collection and use of their information. Meanwhile, a faceless authority continues to change locks and turn off lights. Like Joseph K., victim-survivors "seek acquittal from a crime [they] [have]n't been informed of and from an authority [they] cannot seem to find."[48]

SHOT goes beyond just the problem of data collection to a violation of trust because the information collection and use is conducted by a former intimate partner. Intimate partners reveal things about themselves with the expectation the intimate information will be protected by virtue of the trust relationship.[49] When this trust is violated, it can make the victim feel they were never cared for and emphasize the power imbalance between the two people.

B. Autonomous Functioning Leads to Feelings of Dehumanization and Powerlessness

SHOT significantly overlaps with traditional forms of torture as both rely on producing a sense of powerlessness in the victim.[50] As David Luban explains, torture relies on the dehumanization of a victim by another who uses suffering to communicate the victim is totally under the control of the

---

[44] *Id.* at 1421.
[45] *See generally* Franz Kafka, THE TRIAL (1925).
[46] Solove, *supra* note 41, at 1423.
[47] *Id.*
[48] *Id.* at 1421.
[49] Danielle Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1875 (2019).
[50] I am reluctant to classify SHOT as a form of torture. International human rights instruments have intentionally avoided describing particular acts as torturous to avoid excluding acts that should also be consider torture that have not yet been thought of yet. John Leach, *Psychological factors in exceptional, extreme and torturous environments*, 5 EXTREME PHYSIOLOGY AND MED. at *5 (2016). For example, Article 3 of the European Convention on Human Rights states, 'No one shall be subjected to torture or to inhuman or degrading treatment or punishment,' but the European Court of Human Rights elected not to define torture and refers to Article 3 as a living instrument. *Id.*

perpetrator.[51] Other scholars have described "extreme environments," like prisons, space stations, and abusive homes, where the environmental stimuli are so intense they harms the individual's psyche.[52] This environment is characterized by an individual's lack of control over the environment and, when attempts are made to reduce or eliminate the environmental threats, conditions are deliberately intensified to increase psychological trauma.[53] The worsening of the extreme environmental conditions paired with an intent to inflict psychological distress could be considered torture.[54] SHOT has many of these same characteristics, particularly because smart home devices allow the abuser to non-consensually manipulate a victim's environment and, by extension, them. Like those in "extreme environments," people experiencing SHOT may experience increased intensity in the manipulation of their environment or threat of physical harm by their abusers if they attempt to retaliate by removing devices or kicking the abuser off accounts.[55]

Control over the environment allows humans to not just manipulate their surroundings but to predict future events.[56] Control, as defined by *The Environmental Psychology of Prisons and Jails*,[57] is the ability to regulate one's level of exposure to environmental events.[58] Apparent and perceived control influences how people experience stress and the long-term effects of exposure to stressors, including noise, temperature, and isolation.[59] Privacy is then the ability to adjust one's environment to most closely match one's preferred levels of contact with others.[60] However, an individual needs control over a situation in order to achieve privacy.[61] Inmates in correctional facilities are specifically and intentionally denied such control and stripped of privacy.[62] Loss of privacy can deprive the individual of their sense of self.[63] With SHOT, when a victim loses control over the home, they in effect becomes a prisoner in their own home because they can no longer exert control over the environment and ameliorate their stressors without fear of retaliation.

---

[51] David Luban, *An Interview with David Luban*, 15 GEO. J. INT'L AFF. 110, 111 (2014).
[52] Leach, *supra* note 50, at *2.
[53] *Id.* at *2.
[54] *Id.* at *5.
[55] *See* discussion *supra* Part I.B.
[56] Richard Wener, *The Environment Psychology of Prisons and Jails*, 196 (2012).
[57] *The Environmental Psychology of Prisons and Jails*, the seminal work on building a better mousetrap, analyzes the effect of isolation, light, noise, and control of space on the prisoner psyche. *See generally id.*
[58] *Id.* at 119.
[59] *Id.* at 119–20.
[60] *Id.* at 115.
[61] *Id.*
[62] *Id.* at 118.
[63] *Id.*

Police have been aware of the effects of loss of control and unpredictability and use them in interrogations to illicit confessions. *Criminal Interrogations and Confessions*, the seminal police handbook on conducting interrogations, recommends interrogators seat a suspect away from, but in view of, controls like light switches or thermostats in order to increase their sense of dependence on the police officers with them in the room.[64] This setup also isolates the suspect and removes them from the familiar to increase the suspect's anxiety and trigger a desire to leave the situation as quickly as possible.[65] Abusers similarly use control over the environment to assert control over their victim. By similarly allowing a victim to see the controls which would ameliorate their discomfort but depriving them of the ability to use them properly, the abuser triggers the same feelings of dehumanization present in the interrogation room.

Unpredictable, sporadic stressors have the most negative and long-term effects.[66] One survivor described the use of smart devices against her after leaving her abuser as "jungle warfare" because she could not identify where the attacks were coming from.[67] Because the victim of unanticipated sensory attacks cannot predict, control, or screen the stressors, they then cannot avoid the stressor or become accustomed to it.[68] The stressor is then able to overwhelm a person's psychological defense mechanisms, causing psychogenic shock.[69] Psychogenic shock initially produces acute confusion, which disrupts self-regulation and cognitive processing.[70]

A discrete, disruptive event alone may not have long-term effects. However, SHOT relies on many overlapping disruptive events, each producing psychogenic shock. Each instance uses resources within the supervisory nervous system that would otherwise be used for self-regulation, thus reducing the ability to resist psychogenic shock in the future.[71] When an abuser randomly shuts off the lights or lowers the temperature to fifty degrees and then suddenly raises it, each produces new psychogenic shock in the victim. Each subsequent psychogenic shock then makes it harder to self-regulate and recover from shocks in the future, putting the victim in a constant state of unease and stress.

---

[64] Saul Kassin & Christina Fong, *I'm Innocent: Effects of Training on Judgments of Truth and Deception in the Interrogation Room*, 23 LAW AND HUM. BEHAV. 499, 500 (1999).
[65] Saul Kassin & Gisli Gudjonsson, *The Psychology of Confessions*, 5 PSYCH. SCI. PUB. INT. 33, 42 (2004).
[66] Wesner, *supra* note 56, at 196.
[67] Bowles, *supra* note 5.
[68] Leach, *supra* note 50, at *6.
[69] *Id.* at *8.
[70] *Id.*
[71] *Id.*

SHOT, particularly through the use of smart speakers, can heighten learned helplessness among victims. An abuser could remotely control a smart speaker to loudly play unpleasant sounds at random intervals. Unpredictable, unpleasant environmental effects have been shown to lead to heightened stress and reduced motivation for completing tasks.[72] A 1970s study reviewing the impact of noise on stress found the ability to control and predict noise was more important to determining stress response than the volume of the noise.[73] When exposed to unpredictable or uncontrollable noise, people showed lower levels of persistence in completing tasks when frustrated.[74] Later scholars interpreted this effect as an increased learned helplessness brought on by an inability to influence their environment.[75] For SHOT victims, this disempowerment is magnified by the multitude of devices used.[76] It is not just unpredictable sounds they must contend with but also lights, temperature, and appliances randomly turning on and off. Learned helplessness is then amplified because so many other aspects of the environment are outside their control. This could bleed into other areas of victims' lives leading to decreased social interactions and poor work performance.

These psychological effects are compounded when multiple environmental factors are under attack.[77] In instances of torture, new elements introduced to the process have a multiplicative rather than additive effect on endured stress.[78] An event's stress is better determined by the interactional impact of all events, which is aggravated by the victim's powerlessness within the process.[79] These harms are particularly acute for multi-device homes where SHOT is present. Because the abuser has multiple, simultaneous channels from which to influence the environment, the risks to the victim are heightened and the potential psychological trauma could be severe.

III. NECESSITY OF LEGAL CHANGE

Federal and state laws have been written to address analog, traditional forms of domestic violence and harassment. Even survivor and advocate resources envision technological harassment coming in the form of communication like email, text messages, or phone calls.[80] At present,

[72] Wener, *supra* note 56, at 196.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *See supra* Part I for discussion of multi-device homes.
[77] Wener, *supra* note 56, at 196–97; Leach, *supra* note 50, at *11.
[78] Leach, *supra* note 50, at *11.
[79] *Id.*
[80] *Documentation Tips for Survivors of Technology Abuse & Stalking*, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://perma.cc/SP47-6C94 (last visited Nov. 16, 2020); *Finding*

however, there are no federal or state laws that explicitly criminalize SHOT or regulate Internet of Things devices generally. Prosecutors and plaintiffs must get creative with existing laws regulating analog behavior to tackle the digital counterpart.

A. Federal Statutes

Similar crimes to SHOT, like cyberstalking and cyberharassment, are often prosecuted[81] under the Interstate Communications Act (ICA)[82] and the Federal Interstate Stalking Punishment and Prevention Act (FISPPA).[83] Cyberstalking and cyberharassment are often used interchangeably to refer to harassment or stalking via electronic communications devices.[84] While effective at prosecuting these two crimes, ICA and FISPPA may not be as effective at prosecuting SHOT because these statutes rely on the abuser to have communicated something to the victim to give rise to criminal charges.

The Interstate Communications Act prohibits communications containing threats to kidnap or injure any person, i.e. a defendant must have directly communicated a threat to the victim in order to be prosecuted.[85] This works well for cyberharassment because it typically involves using Internet platforms, like Facebook, Twitter, and email, to contact a victim to relay harmful intent. It might even work well for SHOT if an abuser speaks to their victim through a smart speaker. However, as discussed in Part III.C, the statute's efficacy diminishes when no explicit communication or threat is made.

The Federal Interstate Stalking Punishment and Prevention Act (FISPPA) has less stringent requirements. This statute prohibits a person who 1) intends to harass, intimidate, or place under surveillance 2) with the intent to kill, injure, harass or intimidate 3) from using any interactive computer service to engage in a course of conduct that 4) places a person in reasonable fear of death or serious bodily injury or causes or would be reasonably expected to cause substantial emotional distress.[86] An interactive computer

---

Laws to Charge Perpetrators Who Misuse Technology, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://perma.cc/2N4C-EVVM (last visited Nov. 16, 2020).

[81] Cassie Cox, *Protecting Victims of Cyberstalking, Cyberharassment, and Online Impersonation Through Prosecutions and Effective Laws*, 54 JURIMETRICS J. L., SCI., AND TECH. 277, 279 (2014).

[82] 18 U.S.C. § 875.

[83] 18 U.S.C. §§ 2261–2261A.

[84] Cox, *supra* note 81, at 278. I analogize to these two crimes because they are crimes that the law is effective at prosecuting their analog equivalent while sometimes ignore the unique challenges their electronic counterparts present.

[85] 18 U.S.C. § 875(c).

[86] 18 U.S.C. § 2261A(2).

service is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet."[87] Interactive computer service has been read to include Facebook, Twitter, Google, and other online message boards. This statute would likely be able to target SHOT. Smart devices could be considered "access software providers" because they transmit, receive, and display content.[88] However, as discussed in Part III.C, the intent requirements for this statute have been notoriously difficult for plaintiffs and prosecutors to overcome.

The Computer Fraud and Abuse Act (CFAA) is another possible route for prosecuting SHOT. CFAA imposes criminal and civil liability for unauthorized access to a protected computer. Protected computers include those in interstate commerce,[89] and every computer connected to the Internet is presumed to be in interstate commerce.[90] In the age of ever-connected devices, the question arises—what is a computer? The CFAA defines a computer as any "electronic . . . data processing device performing logical, arithmetic, or storage functions" excluding automated typewriters, handheld calculators, and similar devices.[91] Beyond laptop and desktop computers, "computer" has been read to include cellphones,[92] tablets,[93] e-readers,[94] and videogame systems.[95] It would not take a particularly creative prosecutor to read smart home devices into the definition of a computer. Smart devices are necessarily connected to the Internet and perform computer-like functions including logical (e.g. smart speaker interpreting human voice commands) and storage functions (e.g. smart thermostats remembering temperature preferences; smart locks remembering the appropriate lock combination). It would then appear the CFAA could reach abuses using smart home devices.

However, SHOT is not the type of fraud or abuse CFAA intends to combat. As Solove describes, the American privacy regime is predicated on the Big Brother metaphor of privacy where the collection and uncovering of hidden things is the taboo laws are designed to prevent. CFAA's prohibited conduct reflects this paradigm. It prohibits accessing a protected computer and intentionally obtaining information, obtaining anything of value, committing

---

[87] 47 U.S.C. § 230(f)(2).
[88] 47 U.S.C. § 230(f)(4).
[89] 18 U.S.C. § 1030(e)(2).
[90] *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012); *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007).
[91] 18 U.S.C. § 1030(E)(1).
[92] *Nosal*, 844 F.3d at 1050-51 n.3.
[93] *Nosal*, 676 F.3d at 861.
[94] *Id.*
[95] *Id.*

fraud, or causing damage to the computer.[96] For this access to be criminal, though, the actor must have lacked authorization or exceeded their authorized access.[97] This becomes problematic when prosecuting SHOT. As described in Part I.B, often the abuser is the individual who set up the account, has the passwords for each device, and remains an authorized user on the smart device.[98] Prosecutors then cannot use CFAA to prosecute SHOT because technically the abuser is still the authorized user.[99] CFAA does not contemplate a world in which a computer's authorized user utilizes it against other users of the same device. This renders CFAA a poor vehicle for prosecuting SHOT.

Feriel Nijem's experience with her former partner is illustrative of this problem. Niejem's former partner installed a home automation system he used to "control, punish, and terrify" her.[100] He would turn lights on with a strobe lighting effect and blare loud music at all hours to startle her awake and keep her from sleeping.[101] Despite his manipulation of her environment and threatening calls that included statements like "I am going after the dogs, and then, I am going after you," law enforcement was unable to help because Nijem's former partner was listed as the only owner of the home.[102] It did not matter that Nijem was ultimately diagnosed with post-traumatic stress disorder attributable in part to her experience with SHOT.[103] Because her former partner owned the home, he could do what he liked to control and frighten her from thousands of miles away.

B. State Stalking Statutes

Not every state has laws to prevent cyberstalking, cyberharassing, and online impersonation. Many do not even have laws targeting analog

---

[96] 18 U.S.C. § 1030.
[97] 18 U.S.C. §§ 1030(a)(2), (a)(5)(a), (a)(5)(b), (a)(5)(c).
[98] See discussion *supra* Part I.B.
[99] The bulk of jurisprudence defining exceeding authorization concerns employees. CFAA's prohibition on "exceeding authorized access" has been found to be a restriction on accessing information, not restricting the use of the information accessed. *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012). In a case involving former intimate partners, courts have found a partner did not exceed her authorized access in accessing her partner's computer because (1) the computer was kept in common parts of the marital residence where it could be used by both parties, and thus (2) it was jointly-owned marital property that the parties had mutual access and authority to use. *Sartori v. Schrodt,* 424 F. Supp. 3d 1121, 1126–27 (N.D. Fla. 2019).
[100] Ferial Nijem, *Domestic Violence Survivor Discusses How Smart Home Technology is Used by Abusers to Stalk and Harass*, YOUTUBE (Nov. 2, 2018), https://perma.cc/9PA3-H8D2.
[101] *Id.*
[102] *Id.*
[103] *Id.*

stalking.[104] In this section, I have chosen to review the state stalking statutes of Georgia, California, and Minnesota. I chose these three laws because each represents a different strain of stalking statutes states can adopt.

1. Georgia

A person commits the offense of stalking in Georgia "when he or she follows, places under surveillance, or contacts another person at or about a place or places without the consent of the other person for the purpose of harassing and intimidating the other person." [105] Contact is "any communication including . . . communication in person, by telephone, by mail, by broadcast, by computer, by computer network, or by any other electronic device."[106] The Georgia statute attempts to tackle harassment over Internet platforms by including computer and computer networks explicitly in the definition of contact. Despite this, it falls into a trap common to many stalking and harassment statutes in that it focuses on actor intent or the actor's chosen medium, rather than the victim's response. As described in Part III.C, intent requirements are difficult to prove.

2. California

In California, stalking involves a "person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for their safety."[107] California adds an additional obstacle that plaintiffs and prosecutors most overcome by requiring the actor to have made a credible threat. As described in Part III.C, "credible threat" can be difficult to prove and relies on a direct communication.

3. Minnesota

Minnesota's former stalking statute is the strongest of the three reviewed. Under this regime, stalking meant "to engage in conduct which the actor knows or has reason to know would cause the victim under the circumstances to feel frightened, threatened, oppressed, persecuted, or intimidated, and causes this reaction on the part of the victim."[108] Under the

---

[104] Cox, *supra* note 81, at *3.
[105] GA. CODE ANN. § 16-5-90(a)(1) (West 2020).
[106] *Id.*
[107] CAL. PENAL CODE § 646.9 (West 2020).
[108] MINN. STAT. § 609.749 1 (West 2019).

Minnesota statute, there was no specific proof of intent requirement.[109] The barrier for plaintiffs and prosecutors was thus much lower as they did not need to prove intent to harass. As explained in Part III.C, intent requirements are notoriously difficult to satisfy as both the conduct and the outcome must be demonstrably premediated and intentional. This statute also is technology neutral. It focuses on actor conduct rather than the medium of harrassment, allowing it to be applied both to cybercrimes and physical crimes.

C. Common Statutory Shortcomings

Federal and state statutes share common shortcomings that render them ineffective in prosecuting SHOT. Namely, these statutes tend to require a showing of intent that is difficult to prove or require proof of a "credible threat" that can be difficult to show when abusers are not "communicating" to their victims in manners contemplated by these statutes. While these standards are not necessarily impossible to overcome, every barrier to a successful prosecution makes it less likely police investigate and prosecutors bring suit.

1. Intent

Prosecutors and plaintiffs often have difficulty proving intent in harassment and stalking cases. FISPPA as well as Georgia and California's stalking statutes requires a showing that the abuser specifically intended to harass the victim or intended to place them in fear of their safety through their conduct.[110] The claim will fail unless a victim can show the perpetrator actually intended to cause distress regardless of the actual effect of an abuser's action on their victim.

United States v. Infante illustrates this problem well. In that case, the court found under FISPPA, a defendant must have specifically or knowingly intended to injure, harass, intimidate, or cause substantial emotional distress.[111] Infante met his victim during a summer school class.[112] After the two had returned to their home states, Infante began to contact the victim through a variety of mediums including Facebook, text messages, and phone calls.[113] Infante then flew from his home in Arizona to the victim's home in New York. While there, he followed her but never confronted her.[114] Understandably, this caused her substantial emotional distress. The court,

[109] MINN. STAT. § 609.749 1a (West 2019).
[110] Cox, *supra* note 81, at *4.
[111] *United States v. Infante*, 782 F.Supp. 2d 815, 820 (D. Ariz. 2010).
[112] *Id.* at 817.
[113] *Id.* at 816–17.
[114] *Id.* at 817.

however, found this was not enough to prevail under FISPPA because Infante did not travel to New York "with the intent and purpose" of harassing the victim.[115] Even if the defendant foresees and causes emotional upset, this is not enough to meet the requirement – he must have acted with intent to cause the emotional distress.[116]

It can be particularly difficult for victims of SHOT to prove this intent to cause emotional distress or harass. The court in Infante heavily weighed the fact the defendant never expressed a desire to harass the victim even if his conduct would suggest otherwise.[117] Defendants in SHOT cases could similarly create facially accurate justifications for their course of conduct that a court would therefore not consider harassment. An abuser could say he wanted to get his victim's attention or see if he was still connected to the home devices; all justifications that are not intentional harassment. Compared to *United States v. Conlan*, where the defendant explicitly contacted the victim and made increasingly ominous threats against her safety,[118] victims of SHOT do not have the evidence of communications courts look to when determining intent.

2. Credible Threat

The credible threat standard also serves as a barrier to successful prosecution of SHOT cases. The Interstate Communications Act (ICA) and California's stalking statute both require a credible threat be made against the victim in order to bring a successful case. ICA's credible threat requires "a communication … that a reasonable person (1) would take the statement as serious expression of an intention to inflict bodily harm (the mens rea), and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the actus reu")."[119] In plain language, the government must show the defendant intends to and is able to carry out the threat or a reasonable person would believe they will carry out the threat.[120] California's credible threat requires "a verbal or written threat ... through the use of an electronic communication device, or a threat implied by a pattern of conduct ... made with the intent to place the person that is the target of the threat in reasonable fear for [their] safety ... and made with the apparent

[115] *Id.* at 821. Instead, Infante told law enforcement he had travelled to explore the possibility of pursuing a romantic relationship with the victim. *Id.* at 817.
[116] Cox, *supra* note 81, at *4.
[117] *Infante*, 782 F.Supp. 2d at 821–22.
[118] *See generally United States v. Conlan*, 786 F.3d 380 (5th Cir. 2015).
[119] *United States v. Alkhabaz*, 104 F.3d 1492, 1495 (6th Cir. 1997).
[120] Cox, *supra* note 81, at *5. Rule 4.2: Correct note not referenced.

ability to carry out the threat so as to cause the person ... to reasonably fear for [their] safety."[121]

The credible threat standard has been difficult to meet in cyberharassment cases and is particularly challenging in SHOT cases because there are often no threats to show. Cyberharassment cases may involve thousands of emails, texts, and tweets to the victim, but if not a single one contains a threat, there is no ICA case.[122] In *Alkhabaz*, a defendant posting stories on a message board describing the rape, torture, and murder of one of his female classmates was not considered a credible threat.[123] The Sixth Circuit held a reasonable person would not perceive the communications as meaning to convey intimidation or effect change in a situation.[124] Even if a court were to read manipulating the home environment as a communication, it seems unlikely they would be able to identify a threat in the actions taken because there is no explicit bodily harm being threatened.

IV. COMPREHENSIVE CHANGE

Legislatures are capable of reacting to innovations in domestic violence and harassment as shown by the criminalization of nonconsensual pornography and video-voyeurism in many states.[125] Current inadequacies in the law possibly stem from a desire by lawmakers to govern in an incremental fashion or from our outdated assumptions about what is dangerous or criminal.[126] By amending existing laws and writing new ones, legislatures can address SHOT before the next form of tech-abuse comes along.

Even if you believe prosecutors could read existing harassment and stalking statutes to include SHOT, updating the law could provide clarity to prosecutors and support to victims. First, as will be explained below, harassment is already a low enforcement priority in part because the law is so poorly understood. Making it easier to prove a case might provide prosecutors and law enforcement with the needed incentive to follow up on reports and prosecute cases. Second, criminalizing a behavior signals a commitment to eradicating the harm a behavior can cause.[127] Criminal penalties can serve as focal points for social change and demonstrate societal beliefs about a social

---

[121] CAL. PENAL CODE § 646.9(g) (West 2020).
[122] *United States v. Alkhabaz*, 104 F.3d 1492 (6th Cir. 1997). *See also*, Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 137 (2007). Rule 16.3: Titles of law review articles should be italicized.
[123] *Alkhabaz*, 104 F.3d at 1492.
[124] *Id.* at 1496.
[125] Citron, *supra* note 49, at 1932.
[126] *Id.* at 1938.
[127] *Id.* at 1931.

ill.[128] As Danielle Citron has described it, "law provides expressive clarity, channeling shifts in beliefs, attitudes, and behaviors."[129] Clarifying the law to expressly encompass SHOT would then signal broad support for SHOT victims.

Of course, legislative modifications are not a panacea. Ending domestic violence, including SHOT, requires more than criminalizing one behavior and involves a comprehensive look at the way we construct trust and power in interpersonal relationships. Domestic violence is able to thrive, in part, because society has not fully accepted it as a problem worth pursuing. Approximately eight million women are raped, physically assaulted, or stalked by a current or former intimate partner each year.[130] An average of three women nationwide are killed each day by a current or former intimate partner.[131] These women need societal change, not just legislative.

A. Platform Self-Regulation Is Not Incentivized

SHOT takes place on technology platforms, so it would make some sense to advocate for platform self-regulation. Platforms could easily remove abusers from accounts being used to harass. However, platform self-regulation in this arena is inadequate and disincentivized. Section 230 of the Communications Decency Act gives platforms a broad shield from liability for users on their platforms.[132] Platforms, like Google and Nest, therefore have little reason to get involved in abuses of their devices because there is no risk that those who are being abused would sue them.[133] Additionally, platforms have argued if they make it easier for people to switch who controls the accounts on their products, it is easier for criminal hackers to access the system, providing further reasons for platforms to ignore the abuse.[134]

B. Principles for Updating the Law

[128] *Id.*
[129] *Id.* at 1946.

[130] CTRS. FOR DISEASE CONTROL AND PREVENTION, *The National Intimate Partner and Sexual Violence Survey: 2010-2012 State Report* (2017), https://perma.cc/ELU9-AV42
[131] JUST. STAT., *Intimate Partner Violence: Attributes of Victimization*, 1993- 2011 (2013), https://perma.cc/Z5TU-2GRV.
[132] Citron, *supra* note 49, at 1931.
[133] *Id.*
[134] Bowles, *supra* note 5; Brian Chen, *Here is How to Fend Off Hijacking of Home Devices*, N.Y. TIMES, Feb. 1, 2017, https://perma.cc/X58W-DCLX.

Rather than suggesting particular fixes to the law, I will instead propose broad principles lawmakers should consider when writing new laws to combat SHOT or amending old laws to include it.

First, legislatures should adopt technology neutral definitions in order to combat innovative forms of domestic violence and harassment as they arise. While there may be appetite for technology specific legislative fixes,[135] this model has led to much of the patchwork privacy, harassment, and stalking laws we are currently contending with. Because past lawmakers did not envision a world where your lightbulb was connected to your WiFi, advocates are stuck trying to make definitions meant to prevent telephone abuse fit a more modern problem. A record of communications is no longer sufficient when your abuser can unlock your door as easily as they can text your phone. Writing laws to specifically address SHOT will offer a band-aid when a suture is needed. It may offer relief for a time, but abusers will find ways around the law and weaponize the latest technology in ways that will not fit with the definitions a SHOT specific law would offer. Unfortunately, abuse keeps up with technology. The law should do the same.

Second, harassment and stalking statutes should be amended to remove or lower the intent requirement. Rather than looking to a perpetrators' subjective intent, legislatures could reduce the culpable mental state to one where the defendant knows or has reason to know the conduct would have a particular effect and the conduct does have that effect. Similar to Minnesota's former stalking statute, this language allows prosecutors to go after perpetrators of SHOT because the course of conduct one would reasonably expect to have a particular effect on the victim is present, and it does have that effect. Critics may argue the intent requirement is necessary to avoid frivolous lawsuits and prosecutions, but at present, there is little risk of overenforcement. As described below, law enforcement is not focused on prosecuting or enforcing domestic violence and harassment cases. If anything, removing the intent requirement may encourage prosecutors and police to take domestic violence seriously because it will be easier to prosecute with a reduced intent requirement.

Third, legislatures should not include a threat or credible threat requirement to prove stalking or harassment. Much like the problem with requiring a "communication," threat standards assume a world where harassment is conducted by contacting the victim directly to make a physical threat. The reality of modern day harassment is closer to psychological warfare than physical violence. SHOT victims often receive no threat to their person, if they receive any kind of communication at all. This does not mean they are not being harassed.

---

[135] *See*, Citron, *supra* note 49, at 1944–45.

Instead, to replace both the intent and credible threat requirement while making the law technology neutral, legislatures should focus on the effect on the victim. The Minnesota stalking statute was artfully crafted to center the fear, intimidation, and sense of powerlessness a victim can feel rather than the intent of the abuser. Legislatures could couple the "reason to know" standard with the actual effect on the victim in drafting the elements of stalking or harassment. Words like "frighten" or "intimidate" are broad enough to encompass the kinds of reactions SHOT provokes in victims. Focusing on the effect of the conduct is a more victim-centric approach to governance and could be a show of goodwill to domestic violence survivors and advocates that their concerns are taken seriously.

C. Engineering, Enforcement, and Empowerment

Legislative fixes can be neutered if not accompanied by broader societal change. The following suggestions are not inclusive of all changes that might be necessary but offer a starting point for thinking of a comprehensive societal response to SHOT.

1. Engineering

SHOT relies on not only information asymmetry between the abuser and the victim, but also power asymmetry over control of the device. The power asymmetry is facilitated through the technology's design: the single controller requirement. Even if a device is designed with privacy in mind by allowing multiple accounts on a device or with robust privacy settings, an abuser can deliberately prevent his victim from making use of these features as the device's sole authorized account holder.[136] Because the device favors the authorized account holder with superior rights over subordinate accounts, any other person's rights and access to the device are inherently diminished.

In designing smart home devices, developers should consider departing from the single superior user requirement. Equal or collectivist power sharing among users would remove some of the power asymmetry that currently exists between authorized account holders and other device users. Multilateral sharing would help people become equal partners in the networked home and take some of the power out of SHOT.

[136] Stewart Mitchell, *Tech Traps Domestic Abuse Victims*, PC PROBE 2 (Sept. 1, 2020).

2. Enforcement

At present, law enforcement is ill-equipped to investigate SHOT.[137] Danielle Citron's deep-dive into the use of stalkerware as a tool of domestic violence and harassment revealed law enforcement rarely if ever pursues complaints of monitored phones.[138] Law enforcement also receives little, if any training on the laws and technology needed to investigate these crimes, in part because domestic violence and stalking are low enforcement priorities for police [139] when compared to murder and combatting child sexual abuse materials.[140] Since they do not understand the relevant law, police often advise victims to get rid of their phones without providing additional resources or investigations.[141]

A similar line of reasoning can be applied to SHOT. The law surrounding this type of harassment is murky at best and would be similar to the statutes used to prosecute uses of stalkerware, domestic violence, and harassment. The technology used to investigate is also fairly similar. One can then assume law enforcement receives little training on either the law or technology used to prosecute and investigate SHOT. Additionally, law enforcement priorities have unlikely changed, so reports are likely not pursued as they relate to harassment. Similarly, like advising a victim of stalkerware to simply toss their phone, it is much easier for police to advise SHOT victims to remove the smart devices from their homes rather than actually pursue the leads. This practice reinforces survivors' common belief that law enforcement will not take their complaints seriously.[142]

Law enforcement should be educated on the law and technology available to investigate and prosecute SHOT. NNEDV's Safety Net Project works at the intersection of technology and domestic violence and specializes in training law enforcement on the relevant law and technology to investigate and prosecute tech abuse crimes.[143] The Safety Net Project also convenes a conference each year to discuss updates to the law and discuss techniques that

---

[137] As of December 11, 2020, a search ("Internet of Things" OR "smart home" OR "smart device") AND ("violence" OR "stalking" OR "harassment") yields no results on Westlaw or LexisNexis.

[138] Danielle Citron, *Spying Inc.*, 72 WASH. & LEE L. REV. 1243, 1249 (2015).

[139] *Id.*; *see* Amanda Hess, *A Former FBI Agent on Why It's So Hard to Prosecute Gamergate Trolls*, SLATE (Oct. 17, 2014, 4:23 PM), https://perma.cc/G3A3-NYLK (last visited Nov. 16, 2020) ("Cases that posed a serious risk of physical harm or a significant loss of property were prioritized, as were threats to children.").

[140] Citron, *supra* note 49, at 1929.

[141] Citron, *supra* note 138, at 1249.

[142] *Id.* at 1268.

[143] *The Safety Net Project*, NAT'L NETWORK TO END DOMESTIC VIOLENCE, https://perma.cc/8TUN-HRC4 (last visited Dec. 13, 2020).

have been effective in deterring and investigating technology abuses.[144] These are just some examples of the resources already available to law enforcement seeking education and clarification.

The DOJ can also play a role in combatting SHOT through prosecutorial guidelines, which shape the priorities of the agency and instruct prosecutors on how to interpret the law. Prosecutorial guidelines could supplement, or in dire cases, replace legislation by providing clarity on how prosecutors read existing statutes to combat SHOT. For example, where "communication" is a necessary component of a harassment or stalking statute, DOJ could indicate they are interpreting "communication" to include nonverbal manipulation of the environment, since an abuser could communicate with a device in the home, even if not with the victim directly. By providing broad guidance that any prosecutor at the Department can apply, federal prosecutors could lower the barrier to entry and increase the likelihood SHOT cases will be prosecuted.

3. Empowerment

Empowerment of SHOT and domestic violence survivors is critical for healing and change. Empowerment is a "meaningful shift in the experience of power attained through interaction in the social world."[145] Power shifting has been at the heart of the anti-domestic violence movement from the beginning. Domestic violence gained a name and face in part because women came together to share stories of being controlled partners through physical, psychological, sexual, and economic abuse.[146] The movement recognizes that because abusers relied on taking power from their victims, healing would require restoration of that power.[147] Empowerment in the SHOT context then is about the restoration of control and power that has been taken.

The Empowerment Process Model developed by researchers Lauren Cattaneo and Lisa Goodman describes the iterative process needed to meaningfully empower survivors.[148] First, organizations can help survivors define power oriented goals for themselves.[149] Second, organizations can help survivors carry out actions toward goal achievement.[150] Finally, organizations

---

[144] *Technology Summit*, NAT'L NETWORK TO END DOMESTIC VIOLENCE https://perma.cc/5BJA-DQQ5 / (last visited Dec. 13, 2020).
[145] Lauren Cattaneo & Lisa Goodman, *What is Empowerment Anyway? A Model for Domestic Violence Practice, Research and Evaluation*, 5(1) PSYCH. OF VIOLENCE 84, 84 (2015).
[146] *Id.*
[147] *Id.*
[148] *Id.*
[149] *Id.* at 85.
[150] *Id.*

can help survivors reflect on the impact of the actions taken toward goal achievement as they define new goals, and the cycle begins again.[151] All steps in the Empowerment Process Model take place in the context of using existing community resources, gaining new knowledge and skills, and building self-efficacy.[152]

An organization seeking to apply the Empowerment Process Model for survivors of SHOT might consider the following. First, what interactions with technology does a survivor want to have with technology going forward? What does their future home look like? Second, what knowledge and skills does the survivor already have regarding smart homes and technology more generally? How does their trauma with technology inform resources they can access? Finally, in considering actions to take in furtherance of a survivor's goals, what skills do they want to develop? What are possible unintended consequences (ex. new avenues for abuse) that might result from these actions? Regardless of the survivor's goals or the organization's objective, the survivor's opportunity for choice and control over the recovery process is the most important principle in promoting healing.

SHOT survivors see the benefits to the connectedness and convenience smart home technologies can provide. At the time of her interview, one survivor was in the process of implementing her exit plan to leave her abusive husband.[153] Although she did not know the specifics of the technology or how to remove her husband from the devices, she was excited to take the tech back from her abuser. "I have a specific exit plan that I'm in the process of implementing, and one of my fantasies is to be able to say, 'O.K. Google, play whatever music I want.'"[154]

CONCLUSION

SHOT is just the latest innovation of domestic violence and harassment, a field that inevitably evolves with technology. Advocates are in an arms race against abusers: abusers identify new ways to weaponize technology, advocates identify legal and technological fixes, abusers identify new ways around those fixes. Then, the cycle begins anew.

SHOT deserves recognition as the destructive force it is. We bring smart devices into our homes with the expectation that they will be used to help rather than harm us. Like the washing machines, microwaves, and dishwashers of yore, smart devices stand to offer people immense labor-saving

---

[151] *Id.*
[152] *Id.* at 90.

[153] Bowles, *supra* note 5.
[154] *Id.*

benefits as they evolve. Humanity will not be able to equitably harness this potential if yet another tool of the Digital Age is allowed to continue as a weapon of abuse and control.