Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Types of smart device abuse	The different cases of smart home abuse participants have seen or experienced	**Surveillance**	Surveilling using smart devices	**Location tracking**	Tracking survivor's precise or approximate location		
				Audio/video surveillance	Surveilling the survivor via audio or video		
				Tracking private data	Tracking information like browsing history, watch history, grocery lists, etc.		
		Harassment	Harassing using smart devices	**Manipulating home environment**	Changing something about the home using smart home devices		
				Blocking access to resources	Using smart devices to restrict a survivor's access, or restricting their access *to* smart devices		
				Creating legal problems	Use smart home devices to create legal issues against survivor		
				Misleading survivor	Use smart home devices to project a fake state of the home at one time		
		Suspicion of smart device abuse	Cases where it was not confirmed whether an abuser was indeed misusing smart devices, but where the survivor was scared or worried about smart devices				
Factors that influence smart device abuse	The contextual factors which may influence or lead to smart device abuse	**Abuser access**	The level of access the abuser has before misusing devices	**Shared access**	Abuser has shared access to the device (regardless of who technically *owns* it)		
				Sole access	Abuser is the sole user of the device		
				Unrevoked access	Abuser has access to the device even though they should not anymore		
		Device context	Details about the devices used for abuse	**Device ownership**	Who owns the device? Did the survivor consent to the device being used (if it's a shared device)?	**Survivor owns device**	The survivor is the legal owner of the device
						Abuser owns device	The abuser is the legal owner of the device
						Device is marital property	The devices involved are technically owned by both parties
						Survivor did not consent to device	The device was purchased and/or is used without the consent of the survivor
				Device configuration	Who configures the device	**Abuser configures devices**	The abuser is the one who configures/handles devices, and/or the abuser has sole admin access
				Device intended purpose	What is the purpose of the device, other than for spying/harassment?	**Caring for pets or children**	The device is used to keep an eye on dependents and make sure they are safe
		Tech knowledge	The level of tech knowledge of the survivor and abuser	**Survivor is tech savvy**	The survivor has a decent amount of tech knowledge		
				Survivor is not tech savvy	The survivor is not tech savvy		
				Abuser is tech savvy	The abuser has a decent amount of tech knowledge		
Impacts of smart device abuse	The ways smart device abuse can be harmful to survivors	**Psychological effects**	Smart device abuse creates psychological distress for the survivor	**Sleep deprivation**	Environmental changes prevent the survivor from sleeping		
				Isolation	Survivor is isolated from help, community, information		
				Interrogation	Survivor has to justify their every move		
				Shock	Finding a hidden device is a traumatic experience		
				Can't disconnect	Being connected to the same device as an abuser can show a survivor the abuser's activity even after they leave, which is stressful		
				Paranoia	Survivor constantly worried there are more devices present		
		Financial trouble	Smart device abuse can cause financial issues for the survivor				

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Identifying smart device abuse	Survivors' experiences in identifying that smart device abuse is occurring, either via known devices or hidden devices	**Clues which indicate abuse**	Clues that tip the survivor off that some form of smart device abuse may be occurring	**Clues from abuser**	Abuser's actions indicate surveillance is happening	**Spoken clues**	The abuser says things that indicate surveillance must be happening
						Behavioral clues	The abuser's behavior indicates surveillance is happening
				Clues from device	Device indicates abuse	**Physical clues**	The device shows phsyical signs of surveillance, such as a recording light
						Digital clues	The account associated with the device shows signs of surveillance, such as an access log
						Presence of devices	The presence of devices, in combination with other clues that abuse is occurring, can be enough for a survivor to intuit what is going on
		Challenges to realizing abuse	Challenges to identifying that known devices are involved in abuse	**Mindset around smart devices**	Smart devices aren't seen as a concern and work as intended, you don't expect them to be used maliciously		
				Abuser lies about access	The abuser may lie and say they no longer have access to devices, when they actually do		
				Device is prevalent and widely used	The survivor may find a hidden device, but not realize it is being used to surveil because they think it is theirs. Hard to distinguish malicious device from a benign one		
				No definitive proof	The device does not offer any proof that surveillance is happening		
		Relying on outside resources	Reach out to outside resources for finding devices	**Mechanic**	Ask mechanic to look for tracking devices		
				Technician	Ask technician to look for suspicious router config		
Finding hidden smart devices	Survivors' experiences in uncovering hidden smart devices	**Ways to find devices**	Ways to find devices which may be involved in abuse	**People**	Who is involved in finding devices?	**Survivor finds devices**	Survivor finds devices themselves
						Friends or family find devices	Survivor gets help from friends and family
						Outside resources find devices	The survivor gets help from outside resources to find devices
				Methods	What tools are used to find devices?	**Manual inspection**	Just search manually
						Built-in safety features	Using built-in features like AirTag alerts to find devices
						Find devices by accident	Finding devices without looking for them, e.g, going to the mechanic for something else and they find a GPS tracker
		Challenges to finding hidden devices	Challenges to finding hidden devices that are being used for surveillance	**Device designs**	The designs of devices make them harder for survivors to find	**Devices are hard to find**	The design of these devices does not help survivors find them
						Devices are easy to hide	The design of these devices makes it super easy for abusers to hide them
				Limited methods available	There aren't many methods available, and those that are are not always helpful	**Manual inspection is only way**	There is no other way to find hidden devices except to look for them manually
						Built-in safety features not always helpful	Built-in features may not alert the survivor or may not indicate the exact location of the device
						Built-in safety features not available to everyone	Built-in features are only available to a subset of users (e.g., those with iPhones)
				Outside resources may not find anything	Outside resources can look, but they may not find anything either		

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Strategies for mitigating smart device abuse	Different ways survivors might mitigate or handle smart device abuse	**Legal strategies**	Survivors can turn to legal strategies	**Report to police**	Report smart device abuse to police		
				Get an attorney	Get an attorney to start legal action		
				Judge revokes access	Legally revoke an abuser's access to devices		
				Document incident	This could be through reporting, taking a picture, or other means, to have it on the record somewhere		
				Seek restraining order	Seek a restraining order to kick the abuser out		
				Explore legal options	Not a concrete action step, but looking into the legal options can help someone find next steps, esp. when the legal implications of the abuse are unclear		
		Device-based strategies	Survivors can make changes to the devices involved	**Check all devices**	Make a list of all the devices you own and check each one		
				Change Wifi password	Change the wifi password and get all devices up and running on the new wifi		
				Explore options	Get help figuring out how to make device changes	**Ask manufacturer for help**	Ask manufacturers for clarification on things, like how to remove access or what an abuser's access will be
						Do research	Research yourself what you can do to remove access or something with the device
				Physical changes	Make changes to the physical location of the device	**Disable device**	Remove it, throw it away, unplug it, destroy it, etc. - anything that means the device is no longer functional. Also includes getting rid of a device like a
						Move device	Move the device to a different location, but keep it on
						Leave device in place	Leave the device on and in place
				Changes to account access	Change the digital access an abuser has to the device	**Put account under your name**	For a shared account or account set up by the abuser, change the account to be under your name
						Split shared account	Separate a shared account into two
						Remove abuser's access	In cases where the abuser is logged in, or their device is connected, remove that connection
						Change password to device/account	Change the password to a device or account associated with that device
						Add security	Add security to the account for that device, e.g., adding 2FA
				Reconfigure device	Make non-access control changes to the device's configuration	**Reset device**	Reset the device to factory defaults
						Remove functionality	Remove some of the device's functionality, like muting the microphone
						General configuration changes	It is unclear what specific configuration changes the person is talking about
		Relying on outside resources	Survivors reach out to outside resources for help	**Hotline**	A hotline, such as a suicide hotline		
				VSPs	The survivor reaches out to VSPs		
				Police	The survivor reaches out to the police, not for a specific legal reason or to report, but for help		
		Behavioral strategies	Survivors can make behavioral changes in response to the abuse	**Retreat from tech**	Use technology less in general		
				Assume surveillance	Change behavior with the knowledge that you are being surveilled		
				Wait to make changes	Wait to make changes until you can leave		
				Leave the home	Leave the home shared with the abuser		

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Barriers to mitigating smart device abuse	Barriers to taking action in response to smart device abuse	**IoT-abuse is not isolated**	IoT-enabled abuse usually happens alongside other forms of abuse. Whereas mitigating the IoT abuse on its own might be doable, it can be made more difficult due to the presence of other forms of abuse that are co-occurring				
		Barriers to seeking outside help	Barriers make it harder to rely on outside resources like mechanics	**The results of seeking outside help are unclear**	There are no guarantees when seeking outside help, sometimes due to the variability of people who will help you	**Outcome depends on the person helping**	When relying on outside resources, the outcome can vary a lot
						No guarantees	It is hard to know if the outside resources will be helpful, or if they will be a waste of time
						Possible unintended consequences	It is hard to know what will happen when you reach out to outside resources or know the potential consequences
						Outside resources have limited bandwidth	Resources like a DV shelter have a limited capacity, it may be difficult to get help if your situation is less dire than others who are waiting
				Resources have knowledge gaps	These outside resources are not trained for specifically tech abuse, and may have expertise in only IPV, only tech, or neither	**Outside resources aren't trained for IPV scenarios**	Outside resources don't always know how to help survivors
						Outside resources aren't technology experts	Outside resources (not tech-specific ones, more people like police) are not technology experts
				The survivor's situation prohibits seeking outside help	The survivor may have certian barriers to their particular situation, such as a lack of financial resources or a fear of technology (both of which may have been exacerbated due to the abuse)	**Survivor is worried about tech**	Survivors who are being abused with technology may be less likely to seek services that use tech, e.g., phone-based legal services
						Outside resources can cost money	There can be a charge for using these resources, for example mechanics
		Barriers to legal action	Barriers to taking legal action (e.g., reporting to police)	**Difficult without proof**	Taking legal action is hard when you don't have definitive proof of the abuse.	**Lack of evidence**	There is not enough evidence to prove it
						Evidence from smart devices not helpful	Evidence from smart devices is not always helpful in legal proceedings
						Difficult to prove intent	Even if it's clear that an abuser misused a smart device/if they admit it, they could claim it was an accident or for some other legitimate purpose
				Legal action is often ineffective	Legal action isn't always helpful	**Reactive, not preventative**	Legal action can often only be taken *after* something else happens
						Hard to enforce	Things like restraining orders are hard to enforce in practice
						IoT abuse not a crime	Many forms of tech abuse are, on their own, not technically criminal acts.
						Legal punishments don't consider tech	Even if charges aren granted, tech is not always considered in the resulting order
				Barriers to interacting with police	Barriers to specifically calling the police, reporting to the police, etc.	**Existing barriers unrelated to tech abuse**	Survivors may have many existing reasons not to interact with law enforcement, unrelated to the current abusive situation.
						Police are not trauma-informed	Police assume you always have control over your own home, don't understand the nuances of abusive situations

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
		Barriers to device-based action	Barriers prevent survivors from making changes to devices	**Inconvenience**	It's hard to make changes because of social context, the pain of changing passwords, etc.	**Difficult to un-share**	It's hard to disconnect when you are sharing with someone
						Inconvenient to make changes	It is inconvenient to make some of these changes, like changing passwords or resetting a device (which
				Rules & regulations	You have to follow rules when making these changes, like adhering to property laws or asking the provider first	**Have to ask provider**	For some changes (like splitting a shared account), you have to call the provider to make it happen, and they can say no
						Property issues	The device may be marital property or owned by the abuser alone, meannig the survivor can't remove or change it
						Solutions are illegal	Mitigating abuse requires the use of illegal tools and methods
				Presence of the abuser	If the abuser is present, mitigation is harder	**Abuse could escalate**	If the abuser notices changes or notices that the survivor is researching how to make changes, they could retaliate
						Abuser could undo changes	The abuser could just undo any changes the survivor makes
						Abuser relies on survivor	The abuser may rely on the survivor, making it more difficult to leave or take action
				Device characteristics	Some of the characteristics of smart devices make it hard to take device-based action	**Devices are necessary**	Devices are useful and hard to get rid of
						Devices are expensive	Smart devices are expensive, making it hard to replace them
						Devices are hard to use	It's not clear how to interact with devices, e.g., how to reset them, what to look for
						Tech changes quickly	The devices change quickly, so any information you find online could be out of date or not exactly true anymore
						Devices can have multiple access points	Revoking access might require you to revoke multiple kinds of access, e.g. via the Alexa account vs via Amazon Household
						Don't know how long device has been there	If there is a tracking device on your car, it's hard to tell how long the device has been there
						Devices may inform abuser	Devices may advertise any actions to the abuser

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Strategies to help clients	Actions advocates take to help clients	**Established advocate strategies**	The advocate does typical things they would normally do in a different case	**Safety plan**	Help safety plan		
				Give generic advice only	Advocates provide generic information, but can't really do anything for the client		
				General financial support	Provide the survivor with financial assistance		
		Give specific advice	Tell the survivor specific information or advice which they can take action on	**Recommend documenting incident**	Advocates recommend that the client document the incident, for example by taking a picture of the abuser's name on their TV		
				Tell client what to do	Give the client instructions on how to deal with the abuse. Not making a decision for them, just giving them information on how to do something they want to do		
				Teach survivors about IoT devices and technology	Give the client information on IoT devices and technology that could help them with the situation		
		Direct to other resources	Direct to resources which may be able to help more	**Direct to someone else**	Directing the survivor to an unspecified resource or someone not on this list		
				Direct to legal/government resources	Direct the survivor to people who can help with the legal side of things		
				Direct to IPV experts	Direct the survivor to services tailored for IPV or tech abuse specifically		
				Direct to tech experts	Direct the survivor to tech-focused services: providers, manufacturers, retailers, and mechanics. (Tech including cars here.)		
				Direct to tools and resources for them to use	Direct the survivor to helpful guides or tools that they can take advantage of themselves		
		Do research	Research aspects of the case to try and help more	**Research technical aspects**	Research how the client's devices work and how they could take action		
				Research legal aspects	Research prior cases or statutes related to the case		

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Barriers to helping clients	Factors that make it harder to help clients	**No universal solution**	Solutions must be tailored to each individual situation				
		Do not feel prepared	Advocates simply do not feel prepared to help with these types of cases				
		Hard to research some devices	Some devices, like nondescript tracking boxes, are really hard to find any information on because they are so generic				
		Ability to help is limited	Depending on the situation, an advocate can only offer limited solutions (e.g., if it's over the phone)	**Time constraints**	Advocates work with many clients and have many responsibilities		
				Spatial constraints	Advocates are helping from over the phone or within VSP offices only	**Unable to go to survivor's home**	For example, the advocate is unable to go to the survivor's home to learn about the situation firsthand
						Difficult to help from afar	Advocates don't have a lot of options when helping someone over the phone, e.g.
				Role constraints	Advocates' roles may prevent them from taking action or knowing everything about the case	**Must consider staff safety**	Advocates are limited in what they can do because they need to make sure advocates are not in danger
						Advocates' roles are narrow	Advocates generally cover one specific piece of the situation, like the legal aspects or the shelter aspect. They might not see the whole picture
		Knowledge gaps	There are gaps in advocates' (and sometimes survivors') knowledge that make it difficult to help	**Tech knowledge gaps**	Gaps in the advocates' or survivors knowledge about technology in general	**Advocate is not tech savvy**	The advocate does not have a lot of tech knowledge. This can also include tech like cars. Might split up.
						Advocate is not familiar with devices despite being tech savvy	The advocate lacks knowledge of some devices
						Advocate is tech savvy	The advocate has a lot of tech knowledge
				Knowledge of IoT-abuse specifically	Gaps in the advocates' knowledge about IoT-abuse cases specifically	**Infrequent IoT abuse cases**	These cases don't come up very often, meaning they are unfamiliar
						Limited training	Advocates aren't always trained for tech abuse
						Training is not practical	Advocate tech training doesn't include hands-on components, like actually handling a smartphone or seeing what spyware looks like
						Limited knowledge of resources	The advocate might not know how to help the person themselves, but also doesn't know who to send the client to
						Not sure how law applies	Advocates, even legal advocates, are not always sure how the law applies in these situations
				Knowledge of cases	Advocates may not have all the information about a case	**Limited knowledge of individual cases**	Advocates may only know a small amount about the case, especially when the client is not tech savvy themselves. Often made more difficult because of the volume of cases advocates deal with at one time.
						Don't know the outcome	Advocates don't always know the outcome of the case or whether their advice was helpful

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Suggestions for preventing smart device abuse	Ways advocates and survivors suggest that different stakeholders could prevent smart device abuse	**Suggestions for lawmakers**	Lawmakers should update legislation	**Spying using devices should be illegal**	Legislation should be updated so it is clearly illegal to use smart devices in this way		
				Marketing devices as spy devices should be illegal	It should be illegal to advertise a device for spying purposes		
		Suggestions for manufacturers	Manufacturers need to consider an IPV threat model	**Change device usage policies**	Update the user agreement so that in these situations, the survivor can easily regain access to the devices		
				Consider an IPV threat model	Consider the risks of IPV when threat modeling	**Consider risks beforehand**	Consider the risks of IPV when threat modeling
						Involve stakeholders	Involve survivors and advocates in plans
				Redesign devices	Design devices to better protect against misuse	**Make it easy to reset device**	Make it easier to reset devices when a survivor needs to do that
						Protection against abuse/stalking	Manufacturers should implement protective measures against malicious use of their devices
						Make it easy to revoke access	Make it easy to revoke the abuser's access to a smart device
						Make devices more transparent	Devices should be more transparent about who is connected and what activity has gone on
				Be transparent	Make it easy for people to find information about the device, including how to use it and what the risks are	**Make directions easy to find**	Make it easier to find instructions online for how to reset devices, change configurations, etc
						Present risks of device on the package	Make the risks of the device known at purchase time
		Suggestions for survivor	Ways survivors can protect themselves	**Avoid smart devices**	Don't even purchase smart devices		
				Get informed	Survivors could protect themselves by understanding certain aspects of the device, how it's being used, and tech in general.	**Know how to use device**	Learn how to reset, configure, control the device
						Know how to code	Knowing how to code is a suggestion some advocates have - they connect it with being able to control devices
						Know the risks	Know the risks of a device in your home
						Understand how the partner is configuring the device	Know what the partner is doing to the device
						Know who is using the device	Know the list of people using the device
				Get control	Survivors could take more control of the devices in their home (which may be a hard ask)	**Get control**	Take control of the devices you own (a tall order)
						Get passwords of all devices	Get the passwords for all of the devices so you have control
		Suggestions for resources	Resources which would be valuable in dealing with these cases	**Better training**	Provide training for tech abuse situations. This includes training specifically tor tech abuse, but also training on trauma-informed care generally		
				Accessible & specific guides	There should be specific resources to turn to for tech abuse situations, perhaps organized in a database	**Specific resources to turn to**	Provide specific resources tailored for these types of cases
						Create a database of helpful resources and guides	A database which contains vetted, up-to-date information for advocates and survivors
				Tech services	Services for finding hidden devices, checking devices to see if they are malicious, and serving as expert witnesses to explain tech to the court	**Services for finding hidden devices**	Provide services to help survivors find hidden devices
						Entering the survivor's home	Provide ways to enter the survivor's home, or tools that can act as an equivalent, to get the full picture of what is happening
						Way to identify if device is a tracker	A way to confirm whether an object is a tracking device, for example if a survivor finds a little gray box in their car
						Expert witnesses	Experts who can help explain tech abuse to judges, provide that professional validation

Structural code	Definition	Main code	Definition	Sub-code	Definition	Sub-sub-code	Definition
Barriers to preventing smart device abuse	Barriers which make it harder to prevent this	**Legal opacity**	Manufacturers aren't clear on the legal aspects either				
		Mitigations could be used for abuse	Some changes, like making it easier to revoke a person's access to the device, can also be used against the survivor				
		No way to tell who is who	Devices have no way to tell who is the abuser and who is the survivor, making it difficult to design mitigations that are helpful and also can't be misused				
		Competing priorities / tensions	Different priorities may be at odds with survivor needs	**Theft vs ease of resetting**	Something that is easy to reset is also easier to steal		
				Educating people without scaring them	People need to know the risks, but if we just dump all of the possible ways someone could abuse you with an IoT		
				Ease of use vs ease of abuse	Something that is easy to use is also easy to abuse		
Opinions on smart devices	General thoughts about smart devices	**Positives**	Good things about smart devices				
		Negatives	Bad things about smart devices				
		Double-edged sword	Smart devices are a double-edged sword				
		Impact of these cases	Ways that working on smart device abuse cases impacts opinions of smart devices	**More cautious**	Seeing these cases has made the advocate more cautious		
				Opinion has not changed	Seeing these cases has not changed the advocate's mind	**As cautious as before**	The advocate was already wary of smart devices
						Great when used as intended	The advocate thinks that the devices are still great as long as they are not abused
						Some devices can't do much harm	There are devices which in advocates' opinion, couldn't be very harmful even if others could. For example, a smart coffee maker.
						Not bothered enough not to use them	The advocate is not bothered enough not to use smart devices