Current Challenges of Modern-Day Domestic Abuse

Joe Mayhew and Hamid Jahankhani

Abstract This chapter centres on the emergence of technology in cases of Domestic Abuse using two adjunct parts; (1) how digital coercive control using smart home devices is now an attack vector for abusers and (2) it sets out to highlight the use of a governance model incorporating a risk-based approach following the principles of the Cyber Security Maturity Model (CSMM). Recent reports in the media have identified cases of Domestic Abuse where attackers are using smart home devices to exert coercive control over their partners or former partners. Research importantly highlights a lack of awareness of technology facilitated Domestic Abuse by victims, support workers and law enforcement. This has resulted in the development of a new proposed framework titled SHADA—a Smart Home Anti Domestic Abuse framework, practical challenges and areas of e-policing to better engage stakeholders. The chapter concludes with additional areas of further research and provides an outlook on the use of newer technologies such as AI and considerations for the privacy of citizens in smart societies.

1 Introduction

The evolution of the Internet in the past three decades has restructured the way people communicate in business and private life. Together with the evolution of the Internet of Things (IoT), devices are connecting to the Internet more than ever before. From sensors generating temperature data, asking Alexa to check the weather, controlling light bulbs through a phone application or using a ride sharing app such as Uber to work are only few day to day examples where choices, actions and activities are
being recorded, transmitted and stored, hopefully securely, by the seemingly free technology-driven conveniences [15].

With these innovations, technology and telecommunications companies developing digital and networked solutions have started integrating three technological systems into urban cites: Internet of Things (IoT), cloud computing and big data analytics. With this system integration, the term “smart city” has been defined. As smart cities are driven on the data input of the citizens, this poses challenges to the security and expectations of privacy. According to [11], “capturing Personally Identifiable Information (PII) as well as data about citizens households and linking this data together to create profiles of people, places citizens in order to make decisions about them” [11]. From the legal point of view, privacy breaches are usually covered under the General Data Protection Regulation (GDPR) in Europe and set of privacy laws in the United States (US) [11]. Except privacy issues, there are other security concerns in smart cities. Smart cities are prone to cyberattacks and another issue is the protection of sensitive data after being collected. It has also become evident that manufacturers of “smart city systems” have little or no experience securing their systems.

Cloud data security Authentication and access control are the main security challenges. Data and resources are stored in various services across the internet which can be accessible by any unauthorized person. Therefore, cloud services should have identity management system to authenticating users and services. Access control is key component of data security which authenticate and authorize the users to data and resources which they are allowed to see and use [12, 13]. Access control process is to ensure that users are actually valid users and they have access to the company resources they are trying to access. Authentication is a method which is used to validate the user who is claiming to be and authentication itself is not enough to protect data. It needed another additional layer of security which is authorization which control if user is allowed to access the resources or make any transaction which is being attempted.

Artificial Intelligence (AI) has been a concept that has been part of public discourse for decades, often depicted within science fiction films or debates on how intelligent machines will take over the world relegating the human race to a mundane servile existence in supporting the new AI order [7]. Therefore, the growing use of AI and the speed of its technological advancements may also lead to a lack of understanding regarding security and vulnerabilities that may affect Artificial Intelligence engines.

With the rapid development and deployment of a new generation of artificial intelligence (AI) algorithms and products, AI is playing an increasingly important role in everyday life and is having a significant impact on the very fabric of the modern society. In particular, AI models and algorithms have been widely adopted in a variety of decision-making scenarios, such as criminal justice, traffic control, financial loans, and medical diagnosis [21, 25]. However, a severe security threat to the existing DL algorithms has been discovered by the research community: Adversaries can easily fool DL models by perturbing benign samples without being discovered by humans [19].
The drive to develop smarter cities and smarter societies, will ultimately increase demand for pervasive network access intensifying the necessity for 4G and 5G technology as smart technology relies heavily on access to the Internet. However, this eagerness for further 4G and 5G coverage could have far reaching implications such as making access to the Internet easier for abusers to exert control over their victims from afar.

The term cyber-violence is increasingly working its way into society and refers to repeated abuse committed by one person (the abuser) against a current or former intimate partner through the use of digital technology. The most common methods of harassment and stalking use easily obtainable digital technologies such as phones, tablets, computers and social networking web-sites. With the emergence of smart technologies changing our everyday lives and assisting us to try and live in a more secure and convenient environment, it is being used in reverse as an instrument of psychological warfare on a victim by a perpetrator without any geographical boundaries, [5]. These devices with a connection to the internet, sometimes referred to as ‘IoT’ devices can be remotely controlled and activated using voice commands or smartphone applications such as smart speakers, wearables etc.

Whilst domestic abuse is not a new subject, it has transcended through the years. Although an outdated patriarchal belief, where men were the head of the family and were encouraged to chastise their wives albeit without losing their temper, this was not always the case. Anna Clark, a professor of history at the University of Minnesota discusses domestic violence in a historical sense [2]. In Clark’s paper, she cites work produced by Pomeroy [14], specifically a book titled “The Murder of Regilla” which documents the murder of Appia Annia Regilla Atilia Caucidia Tertulla, born around A.D. 125 and subsequent trial of her husband following the accusation of him killing his wife over a trivial matter.

During the 1950–80s, Domestic Abuse was satirised in comic strips such as those by the twentieth Century cartoonist Reg Smythe, creator of Andy Capp. Smythe styled his character on an English northern wife beater [22].

Modern understanding and acceptance of domestic abuse has changed over the years, the following timeline from the Guardian [20], provides a brief overview of changes in English law since the late nineteenth Century.

The following is a timeline of Domestic Violence Legislation across England and Wales:

- **1860—Law of Coverture**
  - At the point of marriage, a husband became legally responsible for the actions of both his wife and children. This meant he was entitled to use physical or verbal abuse to control their behaviour.

- **1870—Married Woman’s Property Act**
  - Before 1870, when a woman married, her property automatically became her husband’s. After this act, any money she earned or inherited while married stayed hers.
• 1895—Curfew on wife beating
  – This city of London byelaw made hitting your wife between the hours of 10 pm and 7 am illegal—because the noise was keeping people awake.

• 1923—Matrimonial Causes Act
  – This act marked a big change in divorce law. Before, a wife had to prove her husband had been unfaithful and show evidence of other faults. After 1923, adultery could be a sole reason for divorce for women as well as men.

• 1956—Sexual Offences Act
  – This was the first-time rape was defined under specific criteria, such as incest, sex with a girl under 16, no consent, use of drugs, anal sex and impersonation.

• 1961—Contraceptive Pill
  – Contraception was made available on the NHS irrespective of marital status or husband’s permission.

• 1971—The first safe house
  – The charity Refuge opens the first safe house in Chiswick, west London, for women and children fleeing domestic abuse.

• 1975—First select committee
  – A government select committee on violence in marriage is created and recommends a minimum of one family place in a refuge per 10,000 people.

• 1976—Domestic Violence and Matrimonial Proceedings Act
  – This was the first legislation dedicated to combating domestic violence. It gave survivors new rights by offering civil protection orders (injunctions) for those at risk of abuse.

• 1977—Housing Act (Homeless Persons)
  – Women and children at risk of violence were acknowledged as homeless. This meant they gained the right to state-funded temporary accommodation.

• 1988—Housing Act
  – Rents became deregulated making it harder for survivors of domestic violence who tried to escape and find private accommodation. Though some argue it helped by developing more supported housing and refuge services.

• 1989—Children Act
  – The law improved levels of child protection and parental responsibility but mostly ignored domestic violence.
• 1991—Criminal Rape Act
  – Before 1991 it was a husband’s legal right to rape his wife—marriage implied consent for sexual intercourse. This was the first time a woman had legal protection from marital rape.

• 1996—Family Law Act
  – Important changes to this law gave law enforcement automatic powers of arrest where violence had been used or threatened.

• 2003—Inter-ministerial group on domestic violence is established
  – This group received crucial evidence on the scale of domestic violence and use of refuges. Women’s Aid (a charity dedicated to ending domestic violence) played a significant role in providing testimony.

• 2004—Domestic Violence, Crime and Victims Act
  – This made common assault an arrestable offence. This meant that law enforcement could arrest a suspect immediately, rather than leaving them with someone vulnerable while they applied for a warrant.

• 2005—Home Office publishes Domestic Violence: A national report
  – This report was seen as government’s first public commitment to taking responsibility for tackling the issue through policy.

• 2010—Government strategy is set out to end violence against women and girls
  – The strategy developed a 2011 plan which included financial commitments to support rape crisis centres and specialist training for health workers in the treatment of survivors.

• 2014—Clare’s Law
  – A law is implemented across England and Wales giving people the right to ask law enforcement about a partner's history of domestic abuse.

Based on this timeline developed by the Guardian and prior to 2014, the previous 2000 years have focused solely on the physical aspect of abuse in intimate partner relationships. Aside from the obvious fact that mainstream electronic computing has only been around since the later part of the twentieth Century, recent abuse has taken a more intangible path. Exerting abuse through non-physical means, such as mental, verbal or coercive control. This not a new thing, although the medium to inflict this abuse has moved to a more modern, digital attack vector such as through social media, tracking applications or mobile devices or reading personal emails and text messages.
2 Societal Examples

Woman’s Aid, a non-profit organisation devoted to supporting victims of domestic abuse in the UK, describes coercive control as a method for controlling a person in order to make them dependent upon their attacker, through isolation, exploitation and deprivation of the victim’s independence in their normal day to day activities [24].

Woman’s Aid provides a non-exhaustive set of examples of coercive control:

- Isolating you from friends and family
- Depriving you of basic needs, such as food
- Monitoring your time
- Monitoring you via online communication tools or spyware
- Taking control over aspects of your everyday life, such as where you can go, who you can see, what you can wear and when you can sleep
- Depriving you access to support services, such as medical services
- Repeatedly putting you down, such as saying you’re worthless
- Humiliating, degrading or dehumanising you
- Controlling your finances
- Making threats or intimidating you [24].

The CPS (Crown Prosecution Service), admits that signs of coercive control may not be immediately obvious to victims [3, 4]. Dating of this information has provided difficult, although an initial assessment dates it around 2015 or onwards (due to a 2015 case being referenced). The CPS states that domestic abuse takes many forms, typically person to person. However, their advice recognises the use of technology and specifically refers to mobile communications, internet communications (such as email and social media) but also mentions “other web-enabled methods” [4]. There is little more information other than this, but at least there is some mention of it. As this space (and the law) matures, there could be further examples provided along with existing, more well-known methods such as email, texts and social media.

Domestic Abuse, Intimate Partner Violence or Coercive Control can take many discreet forms in a digital setting, the following non-exhaustive list outlines some of the key examples of attack vectors:

- Social Stalking—befriending friends of friends on social media
- Reading emails or text
- Leveraging gifts to children such as mobile phones, laptops or tablets with cameras
- Home surveillance such as Internet connected CCTV
- Smart heating controls
- Smart door entry systems
- Personal Assistants—Amazon Alexa, Google
- Smart lighting controls
- Internet connected home audio systems.
Some of these examples can take place whilst both the abuser and victim are still in the same property.

A high proportion of the other examples can take place once an abuser has left the family home. These could take the form of a victim’s heating being repeatedly disabled during winter and there is no clear reason why. It could take the form of a smart door entry system constantly ringing. Personal Assistants such as Amazon’s Alexa being used to record conversations in the home.

These examples can range from incredibly frustrating, frightening to terrifying for a victim. This is especially so if the victim does not know how to reduce access to these devices remotely, or if the devices were bought and configured by their former partner-come-abuser and removal presents further challenges such as how to remove these devices. In some cases, it may not be possible to remove them and then the challenge of removing access and securing the devices can become an even more difficult situation.

3 Current Challenges and Modern-Day Domestic Abuse

More recently, advanced methods for exerting control in a domestic household has been highlighted through smart home or IoT devices. IoT is primarily a marketing term used for everyday devices connected to the internet so that they can be configured, controlled and/or viewed through a web client (e.g. Internet Explorer, Edge, Chrome or Safari) or application, typically through a smart phone or tablet (another IoT device), [23]. Examples of IoT devices include digital assistants such as Amazon’s Alexa, Google’s Assist, Apple’s Siri or Microsoft’s Cortana; heating controls such as Hive, Nest, or Honeywell; doorbells or digital locks such as those from Ring or Yale and even home audio systems plus many more examples of IoT (fridges, cookers, toasters, coffee machines), the list is becoming endless. With this explosion of connected devices, it is becoming increasingly difficult to keep up to date.

It should be noted that there is an argument that the recent abusive actions—digital coercive control, could be considered advanced, yet they could also be considered a simpler abuse method without the feeling of consequence to the abuser.

Why the argument? Consider the following, the attacks are performed using highly technologically advanced devices that connect to home networks, across the Internet and finally to mobile devices (typically). In between the home automation device and the abuser is a vast amount of silicone, electronics and miles of cabling transmitting and receiving millions of binary ones and zeros orchestrated by millions of lines of software code (culminative). A highly complex mesh of electronics, with the ability to deliver an abuser’s threat payload, inflicting misery on their targets. Conversely, with all of this technology in place, designed, manufactured and maintained by nearly a million IT professionals in the UK alone [18], attackers don’t need to know how to
wire a network, how to setup servers, how to code software. It’s already been done. The delivery medium has already been created for reasons other than for someone to use the technology to inflict abuse towards a victim. The attack could be from any location where there is connectivity to the Internet. Providing there is access, it can be instigated without geographic boundary, without the fear of being caught, or without seeing the misery inflicted and therefore without feeling there are consequences for their actions.

It is in this respect, that it is a simpler method for abusers to cause harm, as technology is that advanced where it creates convenience of actions that previously took a moderate degree of thought and physical presence.

Mobile technologies such as 4G provide an integral medium for abusers with mobile devices and their victims. The pervasive access to the Internet through mobile technology provides a “from anywhere and at anytime” capability for abusers. The additional explosion of media-rich supplying connectivity such as 5G adds a new dimension—the ability to launch attacks in greater frequencies, at faster speeds and in higher volumes.

Consider the ability to exert coercive control through the delivery of larger payloads, such as those to smart TVs, smart home power networks or even electric vehicles. The faster network access and edge computing benefits that 5G provides, could be very well utilised by savvier abusers—or even “abusers for hire” in future smart societies and cities, [5, 6].

Work conducted by the Home Office on domestic abuse and the economic and social costs as a direct result state that in England and Wales in 2016/2017, this cost was c.£66billion [9]. This figure comprises costs to health services, policing, victim services and lost output among many other components. Based on details from the Office for National Statistics, the individual cost per victim equates to £34,015, however this is an average and depending on the exact crime, costs can be significantly more according to the Home Office.

The Home Office states the figure is under-estimated as it does not fully reflect the physical harm that victims sustain.

During the COVID-19 pandemic, reported figures on UK Domestic Abuse resulting in the murder of women by men were approximately double the average for the same periods in previous years [16]. The stress associated with financial concerns, living in close quarters for a prolonged period and uncertainty for the future were all quoted reasons for femicide (and some cases child homicide). The inability to access support services for women during the lockdown were possible reasons for this, although the lockdown presented the unescapable abusive environment, behind closed doors whilst isolated in the home.

In addition, charities reported calls about domestic abuse during the lockdown increased by 120% resulting in nearly 100 arrests per day by the Met police [10]. This highlights two key issues: firstly, abuse in intimate partner relationships can be concentrated during a time where there is no escape for victims when they are stuck in doors for 24 h per day and secondly access to critical support services can be impeded should an abuser withhold access to a telephone or the Internet from a victim.
4 \textbf{SHADA—A Proposed Framework}

There is no straightforward solution to the issue of digital coercive control. Abusers are finding more intuitive ways to excerpt control and abuse their victims. Technology companies inadvertently make it easier to access our homes and a by-product of this is abusers are taking advantage of this. Furthermore, trying to prove any of this is extremely difficult without the adequate awareness, training or guidance.

Analysis of prior research into digital coercive control and interviews with UK domestic abuse charities three solutions can be proposed. When combined, they provide a theoretical framework to support the reduction of Domestic Abuse, specifically in cases of digital coercive control.

The following outlines a theoretical framework based on initial investigations called \textbf{SHADA}: a Smart Home Anti Domestic Abuse framework.

The SHADA framework highlights three key areas based on previous research:

- \textbf{Legislative Amendments}
  - Following research into the UK Domestic Abuse bill, it lacked substance around critical elements such as digital coercive control. As part of SHADA, amendments to the Domestic Abuse bill should include provisions for digital coercive control and protection mechanisms as well as further training and support for law enforcement and support services.
  - There was insufficient information within the Crown Prosecution Services literature that would provide guidance for law enforcement and legal parties. A further legislative amendment would be for the CPS to update their guidance to provide examples of digital coercive control.

- \textbf{The role of Technology Developers}
  - Define a functional standard to provide the ability to easily obtain evidence in the event a smart home device is used in cases of Domestic Abuse.
  - Provide a mechanism for dual management of smart home devices to ensure that no single resident is in control.
  - Consider using a standards-based approach (RFC or ISO) for the SHADA framework that gives confidence to consumers.

- \textbf{Awareness}
  - Campaigns via TV advertisements, posters in social premises and social media aimed to raise public awareness of digital coercive control.
  - Training for law enforcement on how to recognise instances of digital coercive control and methods to collect evidence.
  - Training for Domestic Abuse support staff to help victims identify examples of digital coercive control.
The aims of this framework are:

1. Ensure there is a legal policy is in place to prosecute abusers and protect victims of Domestic Abuse in cases of digital coercive control.
2. Ensure that technology can instil confidence to buyers of consumer electronics for the smart home and that it is difficult to be used in cases of Domestic Abuse without leaving evidence of activity. Potentially using a Kitemark quality standard as provided by the British Standards Institute [1].
3. Raise awareness for
   a. the public to increase prevention,
   b. law enforcement to recognise digital coercive control & collect evidence and
   c. Domestic Abuse support staff to be able and provide appropriate advice.

5 Practical Use and Challenges

The success of implementing a framework such as SHADA relies on an appropriate level of governance and stakeholder engagement across Government, Law Enforcement, Social Services, Public awareness and Original Equipment Manufacturers (OEMs). Applying Cyber Security Maturity Modelling (CSMM) to the framework aligned with stakeholders, can aid in demonstrating the key steps to increasing maturity in society as this drives a risk-based approach highlighting the key controls.

The first stage is to develop a charter and identify the stakeholders and the key outcomes the framework aims to provide. The charter must articulate the who, what and when in the following stages. The charter should provide a clear indication of the stakeholders, their roles and the commitment required within the overall program. The charter should also include the guiding principles of how the program will be governed. First and foremost being the reason why this is here in the first place—to improve the lives of domestic abuse victims and potential victims in the future.

Examples of stakeholders include:

- **Government**
  - Policing: raising awareness on how to support victims and identify and capture abusers
  - Crown Prosecution Services: examples of abuse activities using digital coercive control to better aid convictions
  - Social Services: at the forefront of supporting victims, developing consistent guidance to provide to victims

- **OEMs**
  - The designers and manufacturers of technology can play a crucial part by introducing features that are safer and can increase consumer confidence
• GCHQ
  – Increasing public awareness of digital coercive control, raising concerns of privacy and cyber risk

• Academia
  – Working towards increased research and collaboration, academic stakeholders can provide much needed focus among key questions including.

The second stage would be to perform a risk assessment and identify controls as part of the maturity model. Identifying gaps between current and future knowledge requirements/solutions. Engaging with the stakeholders as part of the process will be fundamental to the long-term success. Support from stakeholders will also aid in the weighting and prioritization of gaps leading to value-driven outcomes that will ultimately improve the situation for victims or potentially reduce the likelihood of domestic abuse in a digital setting.

The third stage requires the development of a roadmap to correct the gaps. Grouped on a per-stakeholder basis, the roadmap should provide a clear set of programs that drive the key outcomes across the framework. Supported by the collaborative work with the stakeholders and the wider public including domestic abuse victim’s and industry support workers. The roadmap should have clear milestones, check-in points and key measurements of success to ensure this meets the desired outcomes.

Finally, the fourth stage is about providing an executable plan that can be delivered back to stakeholders demonstrating how and where to remediate the issues and improve the lives of domestic victims. This plan, developed with the stakeholders, should show the milestones and costs to achieve the outcomes set out in the charter at the beginning of the process. The plan will enable the stakeholders to conduct their own due diligence and have adequate time to review and where required, request funding.

6 E-Policing

The following looks to highlight the lack of awareness and training for the purposes of law enforcement and evidence gathering in e-policing. This is to aid the pursuit of a criminal conviction and protect victims from further harm by deterring abusers.

6.1 Training Requirements

Additional training had been cited as a main area to improve the response from law enforcement and aid them in the identification and prosecution of suspected domestic abusers using technology to excerpt digital coercive control.
The following table provides some examples of the training required:

| Awareness                                                                 | Identification                                                                 | Digital forensics considerations                                                                 |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Examples highlighting changes in abuser’s behaviour                       | How to identify digital coercive control                                      | What evidence could be gathered                                                                   |
| Abusers using CCTV to monitor their victim                                | Victim reports that they receive text messages from their abuser when they    | Subject to appropriate legal documentation, obtain Geo location information of the abuser’s mobile phone |
|                                                                           | immediately return home or leave the home although the abuser is not in the   | Check the local logs of the CCTV system                                                           |
|                                                                           | vicinity                                                                       | With permission of the victim, check their mobile to correlate the time of the messages with Geo location and the CCTV system logs |
| Abuser’s changing smart heating controls of their victim’s home           | Victim reports that heating controls are reset unexpectedly, or dramatically  | Check the heating system logs, some (but not all) provide the ability to track changes              |
|                                                                           | change for no apparent reason                                                  | Check ISP logs for incoming connections to the smart heating system                               |
|                                                                           |                                                                               | Check that the victim’s controller has not been locked out                                        |
| Abuser’s controlling behaviour of smart assistants                        | Victim reports that smart home assistants begin acting strangely such as the  | Check the application log of the smart assistant                                                  |
|                                                                           | default language has changed, there are inappropriate messages being played    |                                                                                                |
|                                                                           | or alerts sounding at unsociable times                                        |                                                                                                |

7 Future Research

Working with support organisations and victims can further increase awareness for law enforcement where feedback on examples of the abuse victims have been experiencing will be invaluable in identifying and pursuing abusers. However, this must be done in a manner sensitive to victims and therefore may not be practical in all circumstances.

One of the key challenges is collecting evidence to pursue a criminal conviction. Evidence could take multiple forms although this could be subject to ambiguity that could be detrimental to securing a prosecution. An example of this is where there are unsuitable examples provided by the CPS as a guide and as such, additional guidance
may need to be sought such as the non-exhaustive examples listed previously that could support law enforcement in these cases.

The SHADA framework in principal, is a hybrid approach that attempts to bridge the gap between the social sciences aspect and the cyber security conflicts of digital coercive control. The SHADA framework could benefit from applying governance controls more familiar to Cyber Security Modelling, a risk-based approach to managing controls in future research.

The following table illustrates an example of this early investigation into the model with specific focus on technical controls to reduce the risk of domestic abuse through digital coercive control:

Former partner leaves the home but still has access to smart devices in the home:

| Risk                                                                 | SHADA component          | Example                                                                 | Risk level |
|----------------------------------------------------------------------|--------------------------|------------------------------------------------------------------------|------------|
| Domestic abuse scenario                                              | Relation to the SHADA component | Example control                                                        | Risk level |
| Unable to access log data on smart home devices                       | Legislative protection   | Mandatory logging of access data held in the vendors secure cloud environment, accessible only with court order abiding to local laws | Medium     |
| Smart home devices are still accessible by a former partner           | Consumer confidence      | Simpler ability to remove access to devices, authorising only those that are permitted | High       |
| The administrative access controls are still in the sole position of the former partner/abuser | Consumer confidence | Dual administrative access to devices by default—e.g. using a two-person rule with potential vendor remote lockout | Medium     |
| Disbelief of the victim’s complaint of digital coercive control by social or law enforcement services | Raise awareness | Creation of training material and mandatory awareness training for social services and law enforcement at a national level to ensure consistency of knowledge transfer | High       |

All of this is fine providing the appropriate level of governance can be applied. This means implementing best practices that can be conveyed to all of society in terms how to detect and protect. The list could become exhaustive, not only because technology moves at unprecedented rates, but because the ability to capture and mitigate all the ways in which technology can be used to exert digital coercive control is a mammoth endeavour.

Further considerations for future research include the fields of Artificial Intelligence, Predictive Analytics and Machine Learning. The application of these newer technologies to devices used in cases of domestic abusive could yeild greater results
for smart societies. Imagine analytics from the applications used to control smart devices with the geo-location data and combining it with Artificial Intelligence could expose abusers using technology for digital coercive control in cases of domestic abuse. This will undoubtedly raise concerns of privacy and the potential for misuse either in a commercial or societal setting. Who owns the data, how could this be used in more nefarious ways, how could we ensure privacy concerns are met—are all these crucial in building public confidence or destroying it?

8 Conclusion

Adapting to the fast-changing landscape of digital coercive control is exacerbated by even faster changing smart home technology in smart societies. Trying to stay up to date with technology is a futile effort as new vendors bring newer products to market and even newer features out quicker and quicker. Part of problem is first recognising that abusers are using smart home technology to coercively control their victims. Recognition that these types of attacks are taking place will provide some comfort to victims, but not much. Secondly, how can this be proven? All things leave some form of digital fingerprint, a log entry or other forms of evidence that can be collected and submitted into evidence.

The SHADA framework provides a multi approach methodology to recognising the issues, creating awareness and proposing amendments to legislation where appropriate. It incorporates a mixed approach as there is no single answer. There is a justification for technology manufacturers to do more and the SHADA framework could give the opportunity to build in features that could provide consumers with increased confidence such as shared administrative responsibilities of smart home devices. There is however, a counter argument that this could mean less security in smart home devices.

This is why the introduction of risk based controls will be the key to driving change, introducing a charter to outline the key milestones, identifying gaps and working with stakeholders such as government, original equipment manufacturers and law enforcement to develop an executable plan with specific outcomes help drive the much needed change which will be a necessity for smart cities and smart societies of the future.

References

1. BSI (2019) BSI Kitemark™. https://www.bsigroup.com/en-GB/kitemark/product-testing/. Accessed 1 Sept 2019
2. Clark A (2011) Domestic violence, past and present. J Women’s Hist 23(3):193–202
3. Conseil De L’Europe (2011) Council of Europe convention on preventing and combating violence against women and domestic violence, 12 April 2011. https://rm.coe.int/168046031c. Accessed 27 Aug 2019
4. Crown Prosecution Service (2015) Domestic abuse guidelines for prosecutors. https://www.cps.gov.uk/legal-guidance/domestic-abuse-guidelines-prosecutors. Accessed 20 July 2019
5. cybersmartcities.com (2018) The overwhelming world of smart cities—cyber-kinetic and privacy threats in smart cities, 11 March 2018. https://cybersmartcities.com/privacy/smart-city-cyber-kinetic-privacy-risks/. Accessed 10 Mar 2020
6. digitalpulse.pwc.com.au (2017) Why we need smart cities, 11 March 2017. digitalpulse.pwc.com.au, https://www.digitalpulse.pwc.com.au/why-we-need-smart-cities/. Accessed 11 Mar 2020
7. Dwivedi Y, Hughes L, Ismagilova E, Aarts G, Crispin Tom, …. Michael D (2019) Artificial Intelligence (AI): multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Int J Inform Manag 101
8. Gillray J (1782) Sir Francis Buller, 1st Bt (‘Judge Thumb’). National Portrait Gallery, London, England
9. Home Office—econ (2019) The economic and social costs of domestic abuse, January 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/772180/horr107.pdf. Accessed 29 Aug 2019
10. Hymas C (2020) More than 4,000 domestic abusers arrested as victims calls to police increase by 30 per cent in lockdown, 24 April 2020. Accessed Telegraph https://www.telegraph.co.uk/politics/2020/04/24/4000-domestic-abusers-arrested-victims-calls-police-increase/
11. Kitchin R (2016) Getting smarter about smart cities. Department of the Taoiseach on behalf of the Government Data Forum, Dublin, Ireland
12. Martin G (2019a) The meaning and origin of the expression: rule of thumb. https://www.phrases.org.uk/meanings/rule-of-thumb.html. Accessed 27 May 2019
13. Martin JA (2019b) What is access control? A key component of data security. https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html. Accessed 16 Mar 2020
14. Pomeroy SB (2007) The murder of Regilla: a case of domestic violence in antiquity. Hardvard University Press, Cambridge, MA
15. Sharma S (2020) Data privacy and GDPR handbook. Wiley, Hoboken, NJ, USA
16. Smith KI (2020). Coronavirus doesn’t cause men’s violence against women, 15 April 2020. Accessed Counting Dead Women https://kareningalasmith.com/2020/04/15/coronavirus-doesnt-cause-mens-violence-against-women/
17. Sommers CH (n.d.) The “Rule of Thumb for Wife-Beating” hoax. https://www.infotextmanuscripts.org/djetc/other_hoff_thumb.html. Accessed 1 July 2019
18. Statistica (2018). Number of employed information technology professionals in the United Kingdom (UK) in 2018, by occupation (1,000 s), 17 September 2018. https://www.statista.com/statistics/778333/information-technology-professionals-employed-uk/. Accessed 22 June 2019
19. Szegedy C, Zaremba W, Sutskever I, Bruna J (2013) Intriguing properties of neural networks. arXiv preprint arXiv 61(99):1312. https://arxiv.org/abs/1312.6199. Accessed 29 June 2020
20. The Guardian Newspaper (2014) Domestic violence legislation in England and Wales: timeline. https://www.theguardian.com/society-professionals/ng-interactive/2014/nov/28/domestic-violence-legislation-timeline. Accessed 27 May 2019
21. un.org (2017) World population projected to reach 9.8 billion in 2050, and 11.2 billion in 2100, 10 March 2017. https://www.un.org/development/desa/en/news/population/world-population-prospects-2017.html. Accessed 11 Mar 2020
22. University of Kent—British Cartoon Archive (2016) Reg Smythe [Andy Capp]. https://www.cartoons.ac.uk/cartoonist-biographies/e-c/RegSmythe_AndyCapp.html. Accessed 27 May 2019
23. weforum.org (2018) 5 big challenges facing big cities of the future, 11 March 2018. https://www.weforum.org/agenda/2018/10/the-5-biggest-challenges-cities-will-face-in-the-future/. Accessed 11 Mar 2020
24. Women’s Aid (2015) What is coercive control? https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/coercive-control/. Accessed 19 July 2019

25. Wu W, Gong K, Huang T (2020) Ethical principles and governance technology development of AI in China. Engineering