Home Security and Emergency Response: The Convenience vs Security Trade-off

Tegg Westbrook[1]

ABSTRACT

The world is increasingly becoming more digitalised as advanced technologies become more affordable and easier to use. Growing digitalisation conjures up many questions about if the "rewards" and added convenience of connectivity outweigh the supposed "risks." Such risks include peoples' overdependency, reliability and trust on technologies to provide safety, security and privacy in homes and workplaces; people's general lack of security consciousness and security hygiene; as well as the (un)suitability of technologies and the strategic use of those technologies to mitigate crime and safety/health risk. Growing "security consumerism" means that nations' citizens now have an important part to play in improving efficiency in emergency response. It is yet to be known, however, whether smart home security appliances are better than passive or monitored alarm systems, and whether added convenience of home automation is supplementary with the security returns. Using a Security Equilibrium Matrix based on literature review and meta-data analysis, this article hypothesises that smart home security appliances provide more security "returns" than passive alarms with the caveat that cyber security and privacy is sacrificed. It argues that the trade-offs between security and convenience is deeply contextual, and this ultimately affects emergency response on a macro-scale. It argues that technology firms have a huge part to play in reducing the variance between the identified convenience-security trade-offs.

Key Words: Smart home security, Alarm systems, Emergency sesponse, Cyber security, Privacy, Convenience.

INTRODUCTION

Market research suggests that smart home security appliances (SHSA) are proliferating at a very high rate in the world (Statista, 2020). Smart home security appliances encompass a range of affordable interoperable "install yourself" technologies including Personal Assistants (e.g. Alexa Guard, Google Home), security cameras, sensors, geofences, light and shade devices, as well as multi-purpose technologies such as "smart toys" and audio and entertainment systems (e.g. incorporated with cameras). This has been enabled by innovations in wireless communication systems, private competition, and affordable and distributable devices produced with low labour costs. They are typically used within the territory of the homeowner, but data can now be shared with trusted neighbours to enable collective neighbourhood safety. Homeowners may also use appliances to keep an eye on disabled or elderly relatives, young children, and pets. Overall, smart home security appliances, used inter-operably, can incorporate up to five "senses" – see (e.g. cameras), hear (e.g. personal assistants), smell (e.g. smoke alarms), touch (e.g. motion sensors), taste (e.g. carbon monoxide detectors) which are inter-operable with Personal Assistants ("tell") or other systems designed to notify homeowners, see Figure 1 below.

[1] Corresponding author: tegg.westbrook@uis.no

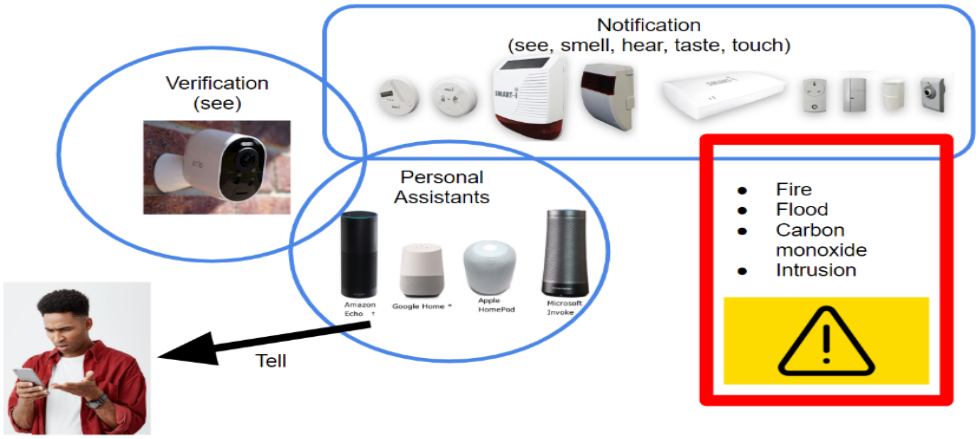

Figure 1: Five Smart Home Security "Senses"

While "security consumerism" and IoT adoption appears to be increasing (Alperovich et al, 2019), global regulatory frameworks for IoT security appliances is fragmentary, with some regulatory frameworks in some countries lacking, whilst others more advanced (ETSI, 2020). Even the most proactive regulatory approaches may lag technological changes, dynamic consumer habits, and criminal adaptations. Academic literature on smart home appliances is largely confined to the computer sciences, and very little attention has been dedicated to exploring the positive or negative societal security impacts of this proliferation, particularly from a theoretical perspective that considers an "equilibrium" of risk acceptance, rewards, issues and faults. Indeed, beyond the possibility that there has been security enhancement in countries where security consumerism is high (Farrell, 2013); various academics, institutions, and media have reported numerous privacy and cyber-security issues with SHSA. For example, Alperovich et al (Abstract, 2019) found that nearly 50% of TP-Link home routers in Eastern Europe and Central Asia have guessable passwords, and in North America, it is 17%. Recent studies have confirmed that consumers are growing more concerned about privacy and data security following numerous media reports of instances of privacy breaches by well-known brands such as Amazon, Google, and Nest (see Agarwal et al, 2020). The use of SHSA has also been attributed to psycho-social issues, for example neighbourhood security appliances conjuring "stranger danger" feelings and racial profiling (Walsh, 2020). On the other side of the argument, some findings have indicated that smart homes and "smart neighbourhoods" have improved security for residents and contribute to speeding up verification of dangers and response times for emergency services (ibid). Investment in home security has been attributed with lower levels of burglaries in many advanced economies (Farrell, 2013). In some areas of the world, such as the USA, security services are working more closely with large technology firms to harness the benefits of wireless infrastructures (Paul, 2019), especially with the ongoing COVID-19 pandemic. This is viewed with alarm by pro-privacy actors who fear the creeping normalisation of mass surveillance. In this respect, other sources point to the issue that collaboration between tech companies and emergency responders has shown no decrease in intrusions in homes (Ng, 2019). Fundamentally, this begs the question about whether security consumerism is offering more rewards than risks to homeowners and making emergency response more efficient and effective.

It is therefore important to understand how the added convenience of home automation is supplemented with added "security returns" for homeowners. Such information will aid scholars and practitioners to understand the opportunities and limitations of smart home appliances, and understand their impact on the safety of homeowners and in terms of improved

efficiency of emergency responders. From an academic perspective, the absence of a matrix that helps to simplify the multi-dimensional issues of digital home security requires dedicated attention. The development and use of a matrix will help us hypothesise the linkage between digitisation, (in)security, risk acceptance, (in)efficiencies, and the sacrifice of normal values such as rights to privacy.

Security Trade-offs

There are three fundamental issues that require addressing in relation to whether security appliances provide an overall "security return" to society: (1) whether smart home security appliances speed up verification and response to safety and security issues better than monitored and passive alarms; (2) whether digitisation is better than other traditional deterrents used in the home; (3) whether cyber vulnerability is an acceptable risk if the rewards and added convenience are much higher.

It is important to first emphasise the differences between passive and monitored alarm systems and smart home security appliances. Passive alarms systems are alarms with no notification mechanism. Passive alarms are often ignored which means that repeatedly there is a slow response to the issues causing the alarm. There are also high rates of "false alarms" – for example, fire alarms being triggered by toasters, or motion sensors triggered by wind. Monitored alarms, on the other hand, are directly linked to a security firm or emergency responders. A faster emergency response is more assured. However, monitored alarms are far more expensive to install and still suffer from false alarms, leading to collateral costs and wasted time for responders, meaning that these alarms usually have to meet certain standards in some countries (e.g. see Salt Lake City Police Department, 2004, National Security Inspectorate, 2020). Many smart home security appliances, on the other hand, which are connected via the internet and communicate to each other via low bandwidth waves like Bluetooth, are designed to detect and notify the homeowner of an alarm activation via their control system. These are more advanced than passive alarms because the homeowner can verify the seriousness of the alarm if, for example, they have visual verification of what is causing the alarm via a "smart camera." It is unknown, however, whether smart home security appliances ensure lower rates of false alarms or whether they speed up emergency response. Many factors can delay a message getting to a homeowner, including the reliability of the internet connection, or simply because the quality of the appliances in the home are of poor standard.

Thus, it is unclear whether smart security appliances are more effective at detecting and notifying of home intrusions and health and safety risks than what is already available on the specialised home alarm market. With regards to home burglaries, whilst smart homes have matured over previous years through the advancement of ICT technologies, it has yet to prove itself over traditional physical deterrents and specialist monitored alarm systems (Brown, 2018). This is despite there being a range of quality systems (e.g. appliances with AI), as well as a higher quantity of systems (cheap and distributed around the home). It also matters about the end-user associations with appliances, with, for example, non-specialists installing digital appliances that might be inadequate, unsafe or unfit for purpose. For example, it has been argued that the vast majority of SHSA contribute mostly to the 'detection' and 'response' elements of a 'defence in depth' strategy (detect, deter, delay, respond), and less so on the 'deterrence' and 'delay' elements (Westbrook, in press). Similarly, many SHSA score relatively low on 'scenario depth', i.e. a spectrum of threats that the security 'layers' – including digital appliances – are designed to deal with. Thus, smart homes may be better protected from some health, safety and security issues more so than others, meaning that more appliances may be needed to mitigate other risks, or more specialist devices and information may be warranted (ibid). Thus, the benefits of digitisation could be fantasy and downfalls might be merely

human-centric. No scaled research so far has tried to identify and, if appropriate, rectify these problems.

With regards to cyber security, there have been many studies that have pointed out the multiplication of entry points in appliances for "tech-savvy" hackers to exploit. Edu, Such and Suarez-Tangil (2019), for example, outline a number of elements that expose personal assistants to various risks, and Jose and Malekian (2015) provide a long list of reasons why homeowners might disregard cyber security. Indeed, cyber security is high on the agenda during the COVID-19 pandemic since many workers are working from home and using less secure devices and applications that what might be available in the workplace. With regards to cybercrime, media and (non-)governmental organisations have warned that criminals are adapting to the challenges that are confronting them and looking for alternative ways to make money. This places more focus on the safeguards and effectiveness of our digital appliances. The impact of "crime displacement" requires more dedicated research, in particular, how home isolation has reduced home burglaries, and how criminals are turning to cyber-crime as a consequence of lost revenues (Europol, 2020). To put it into greater perspective, breaking and entering into residential dwellings have declined, locally and nationally, in some advanced economies (Office for National Statistics, 2020, NSW Bureau of Crime Statistics and Research, 2020, Ashby, 2020). The equilibrant is that cybercrime has increased. In particular, there has been an upsurge of data-harvesting and disruptive malware (Interpol, 2020) which can target smart home devices. There are other well-known motivations for hacking into smart homes that may be more appealing during 'stay at home' periods, including methods to gather information about the occupants, as well as harass and inconvenience homeowners, and enable break-ins (Chang, 2019). Thus, it could be perceived that during the COVID-19 pandemic, our physical property is less likely to be stolen, but our digital property is more vulnerable to theft and exploitation than ever before.

Media and academic attention on the privacy implications of appliances is extensive, but very little has focussed on the balance between the sacrifice of privacy in return for other security returns (see Choo and Sarre, 2015 for legislative and policy dilemmas). Overall, the reason why privacy is challenged in smart homes is because of the heterogeneous, dynamic, and Internet-connected nature of our lifestyles that makes private data more accessible and hence more vulnerable. There is also a lack of "privacy-assured" products because many companies that sell smart appliances benefit in some way by gathering data about the home and homeowner (Molla, 2019). This is in part due to lack of national international standards as well as the will to regulate the industry. Similarly, while consumer demands for better privacy safeguards appears to be increasing (see Agarwal et al, 2020, p. 1), as demonstrated in Mozilla's (2021) "*privacy not included" webpage, privacy-assurance is not a top priority for major brands, leaving little choice to the consumer. Similarly, consumers may state that privacy is a key aspect of their buying choices but may not ensure this (Molla, 2019).

Likewise, some aspects of home security might benefit from using covert security appliances, meaning that visitors and family members might not be aware that they are being surveilled. Indeed, home isolation during the COVID-19 pandemic for many families may have challenged people's sense of privacy between household members and from potential hackers, thus challenging the normal social structures, values and trust that we hold most dear in our homes. Overall, this brings us back the question about whether added convenience, such as improved efficiency and peace of mind, is a sufficient trade-off for sacrificing some values and exposing homes to certain risks.

Understanding how effective and safe smart security appliances are is only a component part to the safety of citizens. However, understanding the opportunities and threats presented by smart security appliances could have a significant impact in mitigating issues (time wasted etc.) experienced by emergency services attending false alarms or attending alarms too late. But these can be influenced by many factors, including infrastructural factors (internet connection in rural areas, for example), systemic issues (quality and interoperability between appliances, technical performance of appliances, the quality of the verification mechanism), appropriate end-use of systems (risk perception of the end-user, strategic and appropriate use of appliances), and the quality of the control system that verifies the homeowner (e.g. push notifications can drain battery power, and therefore are often turned off). Communication issues could mean the difference between attending an alarm on time or too late. The speed of the notification and verification could be influenced by, for example, systemic issues. Blurred images can often be caused by poor internet connection or Bluetooth configuration.

Without dedicated research, the abovementioned issues and questions are based mostly on conjecture. Nevertheless, supposing that smart security appliances score high or low in various "security equilibrium," we can hypothesise whether they provide a "security return." Table 1, below, shows a simplistic matrix of "high" to "low" equilibrium based on qualitative assumptions.

	High Equilibrium	**Medium/Imbalanced Equilibrium**	**Low Equilibrium**
Detection and response	Response has improved. SHSA are similar in effectiveness or better than monitored alarms. Efficient.	Response is more effective than passive alarms, but not better than monitored alarms.	Response has not improved despite proliferation. Inefficient.
Cyber-Security	Smart home appliances leave little or no opportunity for attack or manipulation.	Appliances have some security safeguards, but also some vulnerabilities that are detrimental to overall security.	Many appliances are insecure. They open more doors to intrusion. Counterproductive.
Privacy	Data is anonymised and not shared with third parties. All household members are aware of security appliances in the home.	Some data is shared with third parties. Some appliances offer some safeguards, whilst others do not	All data is shared to third parties without the homeowner's full consent. This data can be leaked and accessed by cyber criminals.

Table 1: Security Equilibrium Matrix

Based on academic and media discussions on smart home security appliances (but with the absence of solid data to inform our decisions), for the sake of advancing this discussion, we can postulate that detection and response, cyber security, and privacy, score a "medium" equilibrium score. Indeed, a large sample testing of appliances in homes, as well as engagement with first responders, and understanding homeowners' cyber security hygiene and feelings about privacy, would be one methodology to undertake. This is not within the scope of this study, however.

If detection and response is "medium" score, and assuming that end-users are using their appliances appropriately, then this would mean overall security enhancement for homeowners with a range of SHSA. Added convenience – though hard to measure – would also be a bonus since this is a primary selling point for the smart home market. If privacy is at a medium score, however, this would mean sacrificing some values. Passive alarms systems do not typically put privacy values at stake because they are not for the purpose of gathering data about the occupants; but this, hypothetically, is to the detriment of a homes' security potential. This means that homeowners (without monitored alarms) need to negotiate a trade-off between (1) less privacy = greater security and safety, or (2) higher levels of privacy = lower levels of security and safety. The contrasts between the former (1) trade-off could be alleviated if, for example, homeowners notify relatives/visitors about the use of security appliances around the home – such as cameras, microphones and other sensors. Fundamentally, this means that privacy in the home is highly contextual for the end-user and indeed based upon the end-user's acceptance that their data is used and shared by the manufacturers of those appliances. Similarly, many homeowners see value in sharing their data if it means receiving targeted and catered marketing material.

What is absent from the discussion is that other appliances that typically do not have a security function (i.e. a feature that detects and/or notifies the homeowner of security issue, or deters criminals from break-in attempts), such as energy monitors, connected taps, refrigerators, kettles etc. – also gather data about us, but in return help us to reduce our energy consumption, control our lights and devices and so forth. Again, the relative low cost of smart appliances might provide a quick return on investment with the end-user's knowledge that they have to sacrifice some privacy and accept some level of cyber risk. The trade-off might be that smart homeowners feel that the risk of cyber-crime and misuse of the data gathered about them is a low risk. Similarly, if the incorporation of security appliances lowers insurance premiums, there are more gains. All told, with cybercrime increasing and burglaries decreasing during the COVID-19 pandemic, 'digital intrusion' may make homes and occupants less safe, at least in the foreseeable future. This means that occupants should consider contextually if the chances of physical intrusion are lowered and if digital intrusion is enhanced.

Based on the matrix, we can conclude that safety and security is enhanced with the sacrifice of our privacy and cybersecurity – i.e. data that is shared with third parties, data that is controlled by one or more household members, or data that is shared with neighbours or even the emergency services. Thus, investing in smart home security appliances is risk-reward calculation for most homeowners. Ultimately, this has an effect on emergency response, and it leads us to question how the smart home sector can influence the shift from a "medium" to a "high" security equilibrium and change the status quo.

DISCUSSION

The idea of home security is changing with connectivity. Advanced security technologies are now more affordable, convenient, easy to use, and can even provide a measurable return – financial or otherwise – for the investment. Digitisation – either with progressive or regressive social and political consequences – has altered the nature of societal security and added more questions than answers about if the "rewards" and added convenience of digitisation outweigh the supposed "risks." Such risks include peoples' overdependency, reliability and trust on technologies to provide safety, security and privacy in homes and workplaces; people's general lack security consciousness and security hygiene; as well as the (un)suitability of technologies and the strategic use of those technologies to mitigate crime and safety/health risk. These sorts of issues bring us to question the role of homeowners in improving emergency response, based on their own abilities to verify the seriousness of alarms before they call emergency responders.

No dedicated study has sought to compare smart home security appliances with passive or monitored alarms, despite the potential to reduce the number of false alarms. Neither have they sought to hypothesise how homeowners might sacrifice some values and expose themselves to certain risks in order to receive certain security returns. Using a security equilibrium matrix, this article has hypothesised that if smart home security appliances score "medium" equilibrium (based on academic and media sources) then smart home security appliances are better than passive alarm systems, with the caveat that some cyber-security and privacy is thereby sacrificed. This leaves a clear message for those who want better cyber security and privacy: they would have to invest in expensive monitored alarms systems *or* sacrifice some level of safety and security by having exclusively passive alarms installed in the home. It therefore concludes that our conceptions of safety, security and convenience, and the trade-offs we make between them, is deeply contextual, and this ultimately has an immeasurable impact the efficiencies of emergency response on a macro-scale.

This leads us to question how we can move – hypothetically – from a "medium" security equilibrium to a "high" equilibrium, which theoretically should lead to safer and more secure homes and businesses. The smart home security sector will need to identify how automated places can reach the level of reliability that monitored alarms provide whilst at the same time reduce the likelihood of false alarms. Likewise, technology firms must leave very little or no opportunity for cyber interference in order to carry more legitimacy in the home security sector. Technology firms must also figure out how data can be better anonymised and how privacy-breaches can be better handled and communicated between different household members and neighbours. The simple conclusion here is that technology firms have a huge part to play in reducing the variance between the convenience-security trade-offs, and thus ultimately improving emergency responses.

REFERENCES

Agarwal, Y., Emami-Naeini, P., Cranor, L, F. & Hibshi, H., (2020). Ask the Experts: What Should Be on an IoT Privacy and Security Label? *2020 IEEE Symposium on Security and Privac*y. Retrieved at: https://doi.org/10.1109/SP40000.2020.00043

Alperovich, G., Case, B., Deepak, K., Dmitry, K., Durumeric, Z., Garg, D., Gupta, R., Kumar, D., and Shen, K. (2019). All Things Considered: An Analysis of IoT Devices on Home Networks. *Proceedings of the 28th USENIX Security Symposium,* August 14–16, 2019,

Santa Clara, CA, USA. Retrieved at: https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak

Ashby, M.P.J. (2020). Initial evidence on the relationship between the coronavirus pandemic and crime in the United States. *Crime Science*, 9(6), 1-16.

Brown, R. (2018). 5G and the promise of a smart home makeover. *Cnet*. Retrieved at: https://www.cnet.com/news/5g-and-the-promise-of-a-smart-home-makeover/

Chang, Z. (2019). Inside the Smart Home: IoT Device Threats and Attack Scenarios, *Trend Mico*. Retrieved at: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios

Choo, K. R. & Sarre, R., (2015). Balancing Privacy with Legitimate Surveillance and Lawful Data Access. *IEEE Cloud Computing*, 2(4), 8-13. doi: 10.1109/MCC.2015.84

Edu, J. S., Such, J. M., & Suarez-Tangil, G., (2019). *Smart Home Personal Assistants: A Security and Privacy Review.* Preprint. Abstract only. Retrieved at: https://arxiv.org/pdf/1903.05593.pdf

ETSI (2020). About Us. Retrieved at: https://www.etsi.org/about

Europol, (2020). *Beyond The Pandemic - What Will The Criminal Landscape Look Like After Covid-19?* Retrieved at: https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19

Farrell, G. (2013). Five tests for a theory of the crime drop. *Crime Science*, 2(5), 1-8. https://doi.org/10.1186/2193-7680-2-5

Interpol (2020). *COVID-19 cyberthreats.* Retrieved at: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

Jose, A. C., & Malekian, R. (2015). Smart Home Automation Security: A Literature Review. *Smart Computing Review*, 5(4), 269-285.

Molla, R. (2019). People say they care about privacy but they continue to buy devices that can spy on them. *Vox*. Retrieved at: https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security

Mozilla (2021). *Privacy not included*. Retrieved at: https://foundation.mozilla.org/en/privacynotincluded/

National Security Inspectorate (2020). *Police Chief's Council (NPCC) Police Response to Security Systems Policy*. Retrieved at: https://www.nsi.org.uk/information-centre/information-for-businesses/police-policy/

Ng, A. (2019). Ring's work with police lacks solid evidence of reducing crime. *CNet*. Retrieved at: https://www.cnet.com/features/rings-work-with-police-lacks-solid-evidence-of-reducing-crime/

NSW Bureau of Crime Statistics and Research (2020). *Crime plummets during COVID-19 lockdown.* Retrieved at: https://www.bocsar.nsw.gov.au/Pages/bocsar_media_releases/2020/mr-COVID-19-crime-trends-in-NSW.aspx

Office for National Statistics (2020). *Crime in England and Wales: year ending March 2020.* Retrieved at: https://-www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2020

Pacheco, J., & Hariri, S. (2016). IoT Security Framework for Smart Cyber Infrastructures. *2016 IEEE 1st International Workshops on Foundations and Applications of Self Systems*.

Paul, K. (2019). Amazon's doorbell camera Ring is working with police – and controlling what they say. *The Guardian*. Retrieved at: https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor

Salt Lake City Police Department (2004). *Verified Response Really Does Work*. Retrieved at: http://www.slcpd.com/wp-content/uploads/multiple_cities_endorse_VR.pdf

Statista, (2020). *Smart Home*. Retrieved at: https://www.statista.com/outlook/283/100/smart-home/worldwide

Westbrook (in press). The Security Depth, System Depth, and Scenario Depth of Smart Home Appliances, International Journal of Reliability and Safety.

Walsh, J. (2020). Ring Doorbells Yield Crime-Fighting Results in Arizona. *Government Technology*. Retrieved at: https://www.govtech.com/public-safety/Ring-Doorbells-Yield-Crime-Fighting-Results-in-Arizona.html

ABOUT THE AUTHOR

Tegg Westbrook is Associate Professor at the Faculty of Science and Technology at the University of Stavanger, Norway. His research interests are in the trade and use of military, security, and police technologies and their social and political impacts. He undertakes research into smart home and city security, perimeter security, satellite navigation systems, autonomous systems, criminology, and counterterrorism.