CYBER SECURITY OF SMART WATCHES : A REVIEW OF THE VULNERABILITIES WITH RECOMMENDATIONS PRESENTED TO PROTECT THE WEARABLES

Aaron James Webb

Macquarie University, Australia

ABSTRACT

This paper will explore the security of smart watches that have seen significant growth over the past few years. As smart watches gain popularity in society, addressing privacy and security concerns to keep sensitive information safe from malicious exploitation must be important. In an industry with limited focus from academic researchers, governments, or leading security companies, I will examine whether smart watches should have mandatory security protection governed by security regulations and policies that protect data privacy and exposure from potential attacks.

KEYWORDS

Security, wireless networks, biometrics, smartwatches

1. INTRODUCTION

Research has shown that consumers are becoming progressively interested in monitoring their health along side an increased demand from parents to provide their children with a GPS tracking device[1, 2]. As a result, smart watches are becoming increasingly important for companies such as Apple, Google, Facebook, and Amazon as they aim to expand their operations into insurance, healthcare, and pharmaceutical markets [3]. As Apple continues to dominate the market with its Watch Series, Google has invested billions of dollars in acquiring smart watch technology companies Fitbit and Fossil, alongside combining with Samsung's Tizen OS to fulfill the gap for an Android-powered smart watch that works seamlessly with all Android mobile devices[4, 5].

This research will aim to identify potential security vulnerabilities and the methods attackers could use to compromise a smart watch. This will bring a new perspective to the literature and highlight the importance of data protection for users to be aware of when using a smart watch and during the risk analysis decision process before adopting a device. Additionally, this paper aims to evoke discussions amongst original equipment manufacturers (OEMs) to evaluate endpoint security protection of smart watches and critically evaluate the most effective technologies available for integration into the device. Finally, this research will aim to encourage governments to champion mandatory security standards and introduce regulatory legislation for the industry to follow.

Security of smart watches has attracted little interest from researchers, companies, or government bodies even though the market has increased by 20% globally YoY, with the amount of data handled by manufacturers intensifying in a fragmented market [6-8]. Industry-leading security

DOI: 10.5121/ijnsa.2022.14304

companies have highlighted that the consumer market for fitness wearables, including smart watches, neglects basic security standards with limited research into the known vulnerabilities to protect users against the risks [9, 10]. The smart watch has seen a dramatic rise in usage since the introduction of the Apple Watch in 2015, changing the market to a more accessible area for the general consumer with sales greater than the traditional watches of Rolex[11]. Along with the major players such as Apple, Samsung, and Huawei, who contribute to over half of the smart watch sales, 40% of the market comprises basic devices with low-level proprietary OS [12]. However, in the age of the Internet of Things (IoT), securing data and privacy rights influences the adoption rate of smart watches, especially amongst healthcare users [13].

2. RELATED WORKS

Recent studies have focused on the technical components of smart watches and the related privacy issues, including several blog posts, reports, and whitepapers [9, 14-18]. One significant remission is the lack of legislation and government regulations to control a market that has grown from a niche industry into a multi-billion dollar market with devices now sold on major shopping sites and reported as a must-have gadget [19, 20]. In addition, a lack of ideas and answers in response to the security vulnerabilities highlighted across academics and organizations is a concerning aspect that manufacturers can freely sell devices to consumers with little care for the user's privacy, basic technology, and data storage.

The literature has been conducted on low-level propriety OS devices, smart watches for children, or wearable devices for the healthcare industry [21-23]. Several studies have researched the security of smart watches for children with similar findings regarding the lack of protection and many vulnerabilities discovered during testing [15, 24]. For example, the Norwegian Consumer Council in 2017, analysed consumer rights in four smart watches marketed to parents to keep in touch and track the location of their children [24]. Key observations highlighted apparent security vulnerabilities in three devices and a general lack of care for users' privacy, with large amounts of unencrypted data sent to servers and third parties worldwide. Advancements to this research came from [15], who researched the vulnerabilities of smart watches for children in Germany and found severe security vulnerabilities ranging from SQL injections to having no privacy statement upon installation of the supporting applications. The authors also discovered that the smart watches tested had no encryption or authentication when communicating with Chinese provided servers or with the supporting application [22].

Research into the adoption of healthcare wearable devices, including smart watches, detailed evidence of a user's perceived privacy risk can influence their decision to use a device, including disclosing personal health information and the potential for data loss[25, 26].The association cannot be exact even though the research into medical wearables and smart watches for children has similarities to the general consumer smart watch, including security concerns around data collection, data flow, and device hardware. Especially considering the smart watches for children have sim card technology and lack key technologies of the consumer market such as contactless payment and activity tracking.

On the other end of the spectrum, little research has been conducted on the security capabilities of high-end devices sold by Apple or Samsung. Instead, researchers focus on the device’s functionality, such as healthcare-related connectivity and users’ privacy paradox when adopting a smart watch [21, 27]. Furthermore, only Apple has a detailed security guide for its smart watch when comparing the manufacturers directly. In contrast, Samsung and Huawei have support forums to answer security concerns. On the other hand, the low-end devices have no manufacturer-supported instructions to assist the user in securing their device or providing an insight into the platform security [28-30].

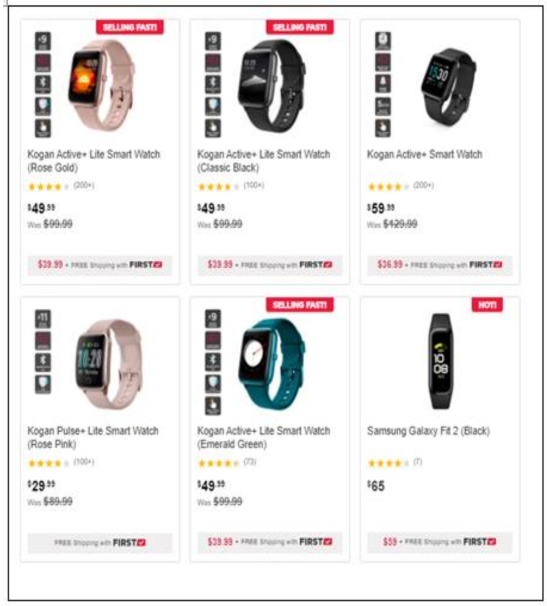
The lack of research into the security of smart watches, the lack of legislation, and the lack of answers to identified issues, therefore, creates an abundance of opportunities for academia, governments, and organizations to prioritize this market with resources and commercial incentives to ultimately protect users from attackers who will no doubt increase their attention onto these devices as the next payout. The extension of the topic, knowledge, and presentation of opportunities will be the main contribution of this paper. In exploring these issues, the following research questions are proposed. Should smart watches have mandatory security protection governed by security regulations and policies that protect data privacy and exposure from potential attacks? Including greater checks for manufacturers to pass before selling devices and penalties for those who sell smart watches that lack proper protection. In addition, should smart watches be manufactured with the technological processing power to house an endpoint security application – like mobile devices and laptops that have applications that offer protection through monitoring and analyzing threats?

3. OVERVIEW OF SMART WATCHES

A smart watch is typically an extension of a mobile phone. Worn on the wrist, the device provides notifications and metrics to the user. Advancements in recent years have seen modern smart watches supporting advanced features and display high-resolution information to the user via a touch screen [31]. For example, devices that focus on activity tracking can monitor, store, and transmit data about one’s activities, such as calories burnt, heart rate, and stress levels. Whereas smart watches are worn by children can monitor location, take photos, and be controlled by parents via an application.

3.1. Smart Watch Market

Apple, Samsung, and Fitbit are the major players in the market. However, new low-end devices that fill sites like Amazon or Kogan see figures 1 & 2, are becoming increasingly popular[32]. Like most low-end technology, these smart watches have been reported to contain malware, intrusive technology, and lack basic encryption standards [15, 23, 24, 33]. For example, Kogan.com has 100s of smart watches for sale from over 45 brands, most of which are Kogan.com branded, as shown in figure 1, for a heavily discounted price compared to the Apple Watch, which retails at $599. It is a similar market on Amazon.com.au, where 1000s of devices are sold from overseas sellers with unknown brand names. Figure 2 illustrates the featured results for smart watches marketed toward children, with many devices containing built-in cameras, GPS tracking, and standalone functionality from sim card-powered technology.


SELLING FAST!
Kogan Active+ Lite Smart Watch (Rose Gold)
(200+)
$49.99
Was $99.99
$39.99 • FREE Shipping with FIRST
SELLING FAST!
Kogan Active+ Lite Smart Watch (Classic Black)
(100+)
$49.99
Was $99.99
$39.99 • FREE Shipping with FIRST
Kogan Active+ Smart Watch
(200+)
$59.99
Was $429.99
$36.99 • FREE Shipping with FIRST
Kogan Pulse+ Lite Smart Watch (Rose Pink)
(100+)
$29.99
Was $89.99
FREE Shipping with FIRST
SELLING FAST!
Kogan Active+ Lite Smart Watch (Emerald Green)
(73)
$49.99
Was $99.99
$39.99 • FREE Shipping with FIRST
HOT!
Samsung Galaxy Fit 2 (Black)
(7)
$65
$59 • FREE Shipping with FIRST

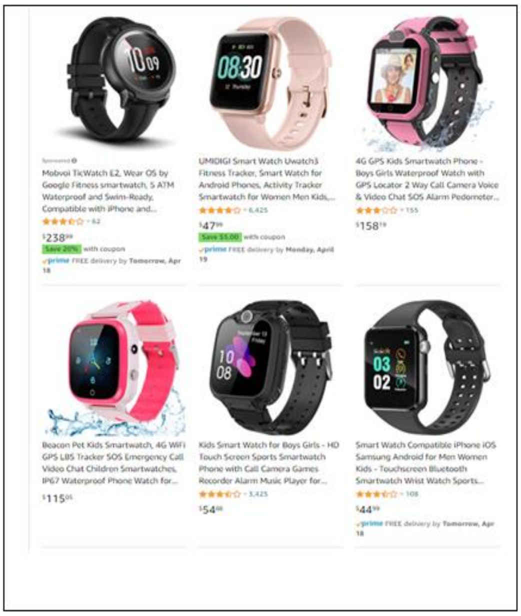

Sponsored
Mobvoi TicWatch E2, Wear OS by Google Fitness smartwatch, 5 ATM Waterproof and Swim-Ready, Compatible with iPhone and...
62
$238.99
Save 20% with coupon
prime FREE delivery by Tomorrow, Apr 18
UMIDIGI Smart Watch Uwatch3 Fitness Tracker, Smart Watch for Android Phones, Activity Tracker Smartwatch for Women Men Kids,...
6,425
$47.99
Save $5.00 with coupon
prime FREE delivery by Monday, April 19
4G GPS Kids Smartwatch Phone - Boys Girls Waterproof Watch with GPS Locator 2 Way Call Camera Voice & Video Chat SOS Alarm Pedometer...
155
$158.19
Beacon Pet Kids Smartwatch, 4G WiFi GPS LBS Tracker SOS Emergency Call Video Chat Children Smartwatches, IP67 Waterproof Phone Watch for...
$115.05
Kids Smart Watch for Boys Girls - HD Touch Screen Sports Smartwatch Phone with Call Camera Games Recorder Alarm Music Player for...
3,425
$54.69
Smart Watch Compatible iPhone iOS Samsung Android for Men Women Kids - Touchscreen Bluetooth Smartwatch Wrist Watch Sports...
108
$44.99
prime FREE delivery by Tomorrow, Apr 18

Figure 1. Smart watches for sale on Kogan.com

Figure 2. Smart watches for children are on sale at Amazon.com.au

3.2. Smart Watch Technology

The technology behind the latest smart watches has created a lifestyle for consumers to access a digital wallet, 24/7 tracking capabilities, and instant access to physiological measurements. Even though the variations are significant, the fundamental hardware powering the devices remains consistent across devices[34].The primary technology includes sensors such as a Global Positioning System (GPS) receiver, Photo plethysmo graphy (PPG) – technology to measure heart rate (HR), accelerometers, gyroscopes, and magnetometers [35-37]. Figure 3 illustrates the process of a user having their activities monitored, then communicated to a smart phone and onto a cloud service which is then fed back to the user via the smart watch display or a smart phone in an easy-to-understand format.

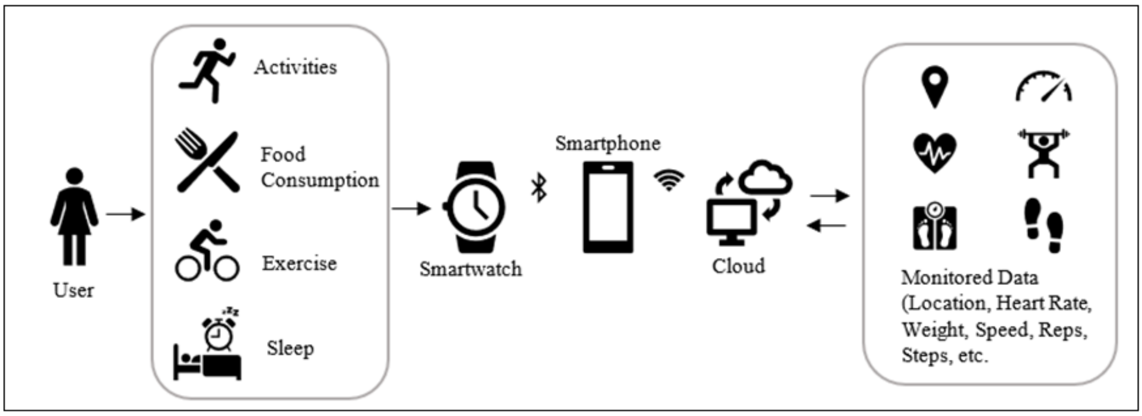

User
Activities
Food Consumption
Exercise
Sleep
Smartwatch
Smartphone
Cloud
Monitored Data (Location, Heart Rate, Weight, Speed, Reps, Steps, etc.

Figure 3. Smart watch tracking and monitoring process

These sensors are essential when tracking health and fitness activities for the user to analyse and improve themselves. However, these sensors have limited computation and processing capability, with devices relying on additional processing units to process the data[38]. Cloud computing technology has provided the opportunity to transmit sensor data to the cloud, which an authorized user can access with any internet-connected device[39].

Advancements in smart watches have introduced Near-Field Communication (NFC) technology for payment services, ticketing, and control hosting access[21]. In addition, cameras and microphones are being built into the device for various uses, including monitoring healthcare patients to examine eating adapts and facial recognition when communicating with doctors [40]. Recently, companies are developing technologies to control your vehicle via a smart watch and even monitor your energy levels while driving for improved safety with adaptive cruise control increasing the distance between vehicles if the drivers' stress levels intensify[41, 42].

Bluetooth technology is a critical component of short-range wireless communication between a smart watch and Bluetooth-enabled devices like smart phones, headphones, or heart rate monitors[43]. The devices formulate a link via a Adhoc network known as a piconet that enables two or more Bluetooth devices to communicate with each other [44]. A master and slave environment is established in the network, with up to seven slave devices able to request and transmit data to the master device [45]. For example, a smart watch would be a slave to the master smart phone; however, a smart watch can also be a master to a heart rate monitor, which acts as a slave. Bluetooth Low Energy (BLE) or Bluetooth 4.0 has been adopted by smart watches as the communication standard due to the low and cheap power consumption to exchange small amounts of data in a few milliseconds[46]. This technology also allows a smart watch to acquire internet connectivity via the master device without establishing a direct internet connection[47].

4. SECURITY OF SMART WATCHES

Like other devices that contribute to the Internet of Things (IoT) environment, a smartwatch is always connected to the internet with data constantly measured and analysed by organizations who either manufacture the device or by third parties who have access to this information [48]. This raises concerns regarding the collection of this data, how and where it is being stored, and how and by whom it is being used[49, 50].

4.1. Industry Overview

Recently, Google's acquisition of Fitbit faced heavy scrutiny from American law enforcement agencies and the Department of Justice regarding how the deep insights into health and location user data tracked by Fitbit would boost Google's market position in the online advertising business [51, 52]. Even though there have not been any significant security attacks on smartwatches, the National Cyber Security Centre (NCSC) and the National Crime Agency (NCA) of the UK have highlighted that hackers can gain easy access to smart watches with reports suggesting ransomware will target devices holding data such as photos, emails, and fitness activities [9, 53, 54]. At a higher level, one major manufacturer of smart watches, Garmin, suffered a ransomware attack in 2020, with a reported $10m payment negotiated to receive the decryption key [55]. Millions of users worldwide regularly use Garmin's technologies to track, store and manage activities, alongside utilizing Garmin Pay for contactless payments. Therefore, this will promote hacking groups to target the manufacturers who store the vast amount of data and increase the pressure on the organizations to pay against the threat of the data being released.

Health information is far more valuable than credit card details and Social Security numbers on the dark web[56]. Therefore, it is not surprising that cyber-attacks on smart watches are predicted to increase with children at risk due to the security flaws highlighted alongside the threat of ransomware attacks on users and manufacturers[56, 57]. The companies selling these devices reap significant benefits by harnessing this data for marketing purposes while seeking technological advancements to promote more user consumption and product identification [58]. However, this ability for smart watches to collect private and sensitive data can increase intrusiveness perceptions and privacy concerns from the user [59].

4.2. Evaluation Against the CIA Triad

From a security perspective, smart watches, like many IoT devices, have limited built-in technology for protecting data and user's privacy. This includes computing power, data handling, storage and communication, and authentication protocols to protect the user[21, 39].The most common information security model to evaluate the effectiveness of providing a secure environment for technology, including smart watches, is the CIA Triad which contains three primary goals of confidentiality, integrity, and availability [60, 61].

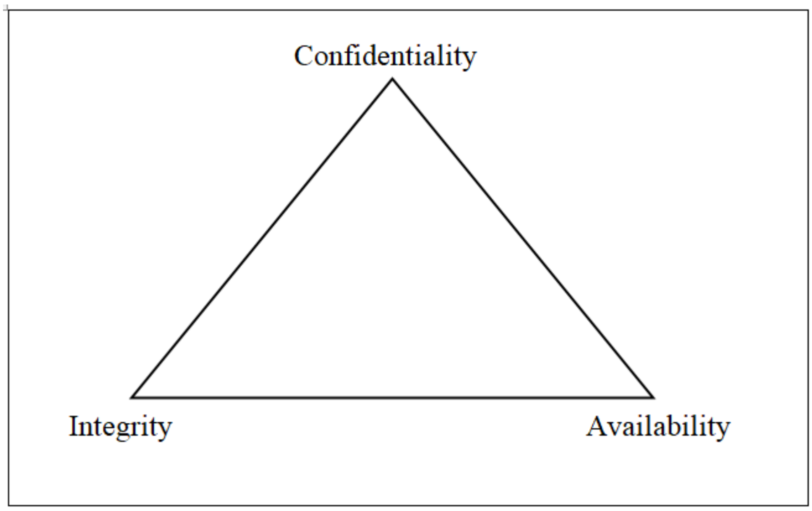


Figure 4. The CIA Triad

Protecting a device's hardware, software, and communication protocols at a basic architectural level ensures clarity in protecting data from unauthorized access, modification, and distribution[62, 63]. Smart watches are no different, with a vast amount of personal information captured. Therefore, the CIA triad can assist with identifying the attributes to focus on, whether it is a risk assessment, asset management, or designing security measures [64].

4.2.1. Confidentiality of Smart Watches

The information on a smart watch is sensitive, containing a variety of data from contact details to text messages, and therefore should be managed securely to avoid unauthorized disclosure or access[65]. The concept of confidentiality is ensuring unauthorized users are actively prevented from accessing specific information while ensuring a secure platform for the authorized users to obtain the information [66]. Firstly, the trusted Registration Authority (RA) performs the initial registration process of the user via the device, smart phone, and cloud server, with the information for various authentication steps such as passwords stored in these devices [67]. Smart watches have limited computation power, and therefore once the device starts collecting data from heart rate to location, this information is sent to the smart phone and onto the cloud server for detailed analysis and storage. A typical smart watch supports two types of authentication: local authentication, which is secure communication between the device and smart phone, with the second being remote authentication between the device and cloud server [68].

Smart watches rely on BLE as the communication method to exchange data between devices. However, as with any other form of wireless communication, the security of Bluetooth has vulnerabilities and emerging threats [46]. One weakness relates to the malicious intervention when pairing devices due to flaws in the required trusted link key establishment protocol and how session encryption is not mandatory [69]. This allows attackers to eavesdrop on the pairing and authentication process, then use a brute force algorithm to identify sensitive information such as a PIN, or attack using Man-in-the-Middle (MITM) intrusion as authentication is achieved without a shared secret key [70]. As a result, the attacker can trick the devices into believing they are paired when in fact, they are paired with the attacker, who can read all traffic as it passes between the parties, including login credentials and personal information [60, 71].

Proposed ideas have been presented to design a greater secure authentication model for smart watches and address confidentiality issues. Firstly, the authors[14] presented a lightweight anonymous authentication scheme using cryptographic operations to protect message transmission while ensuring that smart watches' limited storage and computation capabilities are not impacted. Secondly,[67] presented a lightweight authentication protocol for a range of smart watches to address manufacturers' power usage challenges due to the lack of processing power and battery life within smart watches. The authors highlighted an environment with low computation cost to operate one-way hash or symmetric critical cryptographic operations as a potential method of maintaining user confidentiality. Authors[72] introduced a novel asymmetric three-party-based authentication scheme using a QR code, visual out-of-band (OOB) channel, and human intervention during the authentication process. Although the authors highlighted that the model could be time-consuming, they reported resistance against man-in-the-middle and eavesdropping attacks. Finally, a handwaving authentication method was tested to provide secure access to devices via analysing the user’s biometrics to extract behaviour feature[73].

4.2.2. Integrity of Smart Watches

The integrity security requirement is an essential component to mitigate against the threats of malicious or authorized bugs within the device or network, which involves protecting information captured from degradation or illicit manipulation either at rest or in transit[74, 75]. Unfortunately, even though the integrity principle is a critical goal of the CIA Triad, there is limited research into the direct integrity exploitation of smart watch devices, which has been acknowledged as a limitation for this section. I will, however, provide examples where integrity objectives can be applied, albeit from an indirect perspective.

Author [76]highlighted examples of compromising the data when in transit to the cloud due to devices lacking sophisticated secure data flow. For example, in 2020, UK-based security firm Pen Test Partners discovered a flaw in low-end smart watches that allowed anyone with basic hacking skills to send fake pill reminder notifications to targeted dementia patients[77].Vulnerabilities were found in the supporting software system called SETracker, which lacked any authentication or authorization when sending commands server-to-server. In 2014, researchers were able to attack a Samsung Gear smart watch using a brute-force attack on the PIN, exploiting the link messaging protocol, to access the user’s data which can be decoded to view Facebook conversations[17]. Fortunately, the Trusted Execution Environment (TEE) found in smart phones to enable protection from untrusted apps or malware is starting to be ported on devices such as the Samsung Gear S2 and S3, which contain the Knox security platform[21]. This segregated environment protects the integrity and confidentiality of the data from other software that reside outside of the TEE [78].

4.2.3. Availability of Smart Watches

Availability is the concept of how information can be accessed by authorized users in a timely and reliable manner[79]. The smart watch market had an initial focus on capturing a user's data while running due to the early GPS tracking capabilities in the early 2000s but has since evolved to a device that features contactless payment, Bluetooth technology, and personalized information that can reveal passwords, daily routines, and credit card transactions[80, 81].Smart watches are becoming increasingly self-sufficient in managing and tracking information while ensuring availability for data access, whether it is on the device directly or via a third-party management application like Strava [82].

Essentially, the backend servers and networks should be available 24/7 for the authorized user to access their information whenever they want to. The only known availability breach relates to the ransomware attack on Garmin, which forced a shutdown of its infrastructure, including the Garmin Connect service, which contains the users' data [83]. Even though no major security breach from a smart watch has been detected, the advancements in the technology allow for more sensitive data to be captured by users in a digital, remote working environment, leading to availability breaches from lost or stolen devices, especially when a smart watch is unencrypted or lacks password protection[53, 84]. This can lead to similar examples of when an MI6 laptop containing sensitive information was left in a taxi or the theft of a laptop from an employee working for a healthcare organization [85, 86].

Research in 2015 focused on the availability of healthcare data on connected devices for diabetic patients and found a reduced state of data availability [87]. Although the research looked broadly at medical devices, it highlights an essential principle for the smart watch industry: handing over control to the devices from a medical perspective should be addressed with caution. Especially when healthcare professionals rely on smart watches to remotely capture patient data, and the major technology players are expanding their operations into this space [3, 40]. Finally, policy updates from Samsung have terminated the Get Location Service for its Galaxy Watch range, creating an availability concern for users that previously relied on this service to locate lost devices [88].

4.3. Legislation

As mentioned, this industry lacks mandatory legislation, including the design, manufacturing, security tests, and data storage controls. This has led to many experts expressing concern about the lack of regulatory structure for industry compliance within a market known for poor device security, with 90% of malicious cyber botnets targeting IoT devices [89]. Therefore, this section will highlight several legislations that relate to the use and management of smart watches.

The Australian Cyber Security Centre (ACSC) published an IoT security code for manufacturers to follow with 13 principles outlined to ensure better protection for consumers[90]. The code of practice includes providing detailed privacy policies and adopting encryption methods when storing credentials. However, these principles are voluntary and cover the IoT devices from a broad-spectrum approach rather than specific guidelines for each device under the IoT umbrella [91]. One notable remission is how the guide focuses on the devices and not the associated backend server - stating how backend servers should follow and implement their respective practices. Against other IoT devices, smart watches track considerably higher amounts of personal data stored in servers around the world. Therefore, the lack of inclusion from the ACSC to provide principles for data management of IoT devices is a major concern.

All smart watches contain a vast amount of health data captured by the manufacturers and handled against weak policies written without mandatory regulatory compliance or adherence to legal frameworks such as the Health Care Portability and Accountability Act (HIPAA)[92, 93]. HIPAA does not protect the health and fitness data captured by smart watches or fitness apps, such as the amount of exercise an individual has completed or their heart rate levels throughout a day[94]. Therefore, if the device manufacturer sells or passes on the individual's data to a third party that falls outside of the HIPAA listed entities, they are not breaching the privacy rules, nor will the data be under HIPAA protection [95].

Under HIPAA, protection is only provided for individually identifiable data and not the re-identity of data which is easily achieved due to the advancements in technology [92, 94]. HIPAA was introduced in 1996 when the re-identity of data was difficult to achieve. However, the expansion of data points from a range of sources has made it easier to re-engineer data and link it back to an individual [96]. The Safe Habor Method and the Expert Determination Method of de-identification are authorized under the HIPAA Privacy Rule. However, research has shown that re-identification was possible through gathering datasets from online sources[97]. This highlights the importance of robust data governance principles and the urgent need to uplift the HIPAA Privacy protection.

The U.S. Agency, The Food and Drug Administration (FDA) classifies smart watches into a low-risk category and, therefore, would not require regulation under the recommendations of the FDA[98]. This low-risk classification allows manufacturers to seek clearance for technological advancements without a formal approval process or extensive testing, such as the latest heart-monitoring app from Fitbit, which tracks irregular heartbeat [99]. However, allowing new data tracking applications to be published without challenge is a concern that should alarm users that the technology monitoring their health has not been approved or tested by government bodies.
Bluetooth security protocols have guides and standards from The National Institute of Standards of Technology (NIST) and The Institute of Electrical and Electronics Engineers (IEEE). For example, NIST 800-121 R1 lists recommendations including the authentication, confidentiality, and authorization over the information, whereas IEEE 802.15.1 provides Bluetooth security standards surrounding the technology of low power, low data-rate exchanging devices [43]. These publications are encouraging to see, which provide recommendations for guiding users on Bluetooth security of smart watch devices.

The potential use of smart watch data as evidence in litigation has brought experts to push for new regulations to protect employees' health and fitness data within employment legislation [94]. Researchers have presented various models to protect data availability, including [100], who introduced a tool called GearGadget for law enforcement and analysts to extract data from Samsung Gear S3 in a secure environment while outputting MD5 hash values for data verification. In 2016, prosecutors were able to extract data from an Apple Watch to charge a 26-year-old with the murder of her grandmother in Adelaide [101]. The investigation presented the activities and heart rate measurements from the grandmother who was wearing the device to contradict the defendant’s version of events accepted in the court. With the increased popularity of smart watches, extracting data from the devices will become more prevalent in legal cases to provide critical evidence. Therefore, attention is required by manufacturers and regulators to assure the confidentiality, integrity, and availability of smart watch data when used as evidence.

Finally, in 2016, the European Union’s General Data Protection Regulation (GDPR) introduced comprehensive requirements for businesses, including smartwatch manufacturers like Apple, Samsung, and Fitbit, to present clear privacy policies informing the user of the processing and use of captured data [102]. The most popular smart watches have well-rounded privacy policies, with Apple applying similar policies for the iPhone and Watch, with the likes of Samsung and Garmin offering simple steps to delete your data [103]. Fitbit provides information on its privacy policies, but it is unlikely the user will read or even understand them [92]. However, as mentioned, Google's acquisition of Fitbit and merger with Tizen have raised questions over the use of data captured by smart watches [4, 93]. GDPR requires users to be informed if data sharing is planned, but the policies' ambiguity and a lack of requirements against today's data extraction methods create loopholes for organizations. For example, Google could extract the health and lifestyle data from their smart watch entities to help build their new insurance operations, giving them a competitive advantage over organizations that do not have this wealth of information[104].

Article 9 GDPR describes the misuse of biometric data for the sole purpose of identifying an individual and data concerning physical or mental health [105]. As a result, in the context of smart watches, the scope of health data is broad, with most data collected from a device falling under this category [106]. In addition, under Article 9.2.C., data processing is allowed when it is in the best interest of a patient who is physically or legally incapacitated from given consent, with fines imposed on those who refuse to provide medical information [107]. This exemption applies to health professionals. However, loopholes in GDPR allow an employer to access an employee's health information captured by a smart watch if they can show that processing this data is necessary for preventive and occupational health [108].

4.4. Summary

Smart watches have introduced many conveniences for the user, with the benefits of data access and functionality overestimated against fundamental privacy issues [109]. The increased features have created a society where users freely track and store their personal health information on the cloud storage servers without second-guessing the unique value of this data and using the available settings to protect their privacy [18].Current smart watches are small, entering passwords is very time-consuming, and the decision to purchase one to gain convenience overlooks privacy. Even though users claim to be concerned about privacy, many ignore the concept of purchasing a device [110]. This disparity between behaviour and claimed concern is known as the Privacy Paradox [111]. As a result of this abundance of sensitive information stored against little security protection, smart watches are becoming an increasingly attractive target for attackers to exploit.

4.4.1. Summary of Common Vulnerabilities

Gaining access to a user's data can be achieved via brute force or physical theft of the device and simply using the device without any barriers due to the lack of password protection and 2FA. Smart watches have limited storage space with data uploaded to brand-specific or open cloud-based servers worldwide without strong local or remote authentication measures to protect against unwanted access[34]. A lack of awareness regarding the commercial and legal usage of data generated by smart watches is evident, alongside a general unknown over what type of information is tracked and who has access to it[92]. Social norms, emotions, and conveniences are valued greater than the privacy concerns acknowledged by users[16].

Several studies have highlighted how manufacturers target children with affordable smart watches with built-in cameras, GPS tracking, and communication technology but lack clear security protection [1]. These devices have no supporting privacy statements, encryption, or authentication and are open to attacks like SQL injections [15, 22, 24]. However, the biggest issue is weak default passwords (123456), supporting smartphone applications and key software platforms[17, 77]. The lack of computation power requires traditional memory-based authentication methods like PIN to be widely adopted due to the small screens making long passwords an inconvenience to use[112]. However, PIN authentication has several weaknesses, including being susceptible to shoulder surfing and reconstructing biometric movements to capture the sequence of digits [113]. Additionally, the lack of encryption within the trusted link critical establishment protocol pairing process leaves smart watches open to eavesdropping and MITM attacks [69, 70]

4.4.2. Summary of Mitigation Measures

As a result of known vulnerabilities, China's Army banned smart watches due to the potential for devices to be hijacked as eavesdropping tools to exploit sensitive locations, communications, and military secrets [114]. Then in 2020, the National Cyber Security Centre (NCSC) of Great Britain proposed a ban on smart watches until the identified security flaws are fixed by the manufacturers[115]. At a technological level, utilizing the Trusted Execution Environment of paired smart phones and introducing greater authentication protocols has demonstrated resistance against known vulnerabilities[21, 72, 73, 78]. However, highlighting the issues and critically evaluating the vulnerabilities is insufficient to change behavior [116]. Nor does legislation provide much incentive for the user or manufacturer to change their behavior, especially when codes are voluntary to follow, have broad definitions, or are classified against minimal controls[91, 98, 106]

5. DISCUSSION

This research paper aims to identify potential security vulnerabilities of smart watches and examine the technical and legislative advancements required to reduce exposure to malicious activities and protect users' data privacy. The methodology criteria analysed a broad range of databases and journal publications from the previous ten years that presented findings on the security of smart watches from both a technological and psychological adoption approach. The findings showed that research conducted on smart watches illustrated several security flaws across various consumer devices, especially those marketed at children. Consistent findings proved that more research is required with greater levels of involvement from the government and increased user awareness. However, the lack of literature failed to provide clear evidence that all smart watches have security vulnerabilities, notably the high-end devices, which account for a significant market proportion.

Overall, the findings confirmed that many smart watches operate within an unsecured environment that rely on critical infrastructure to control wireless sensor networks (WSNs) that send and receive sensitive data. Even though this infrastructure poses data protection flaws, advancements to improve the security of smart watches have started to be published with similarities in the message to provide awareness for the industry. It is essential to view the security of smart watches in the IoT environment with similar methods adopted for all devices[117]. Users need to trust their data from an end-to-end perspective, ensuring the convenience and functionalities of smart watches continue to be beneficial while knowing that strong security standards and practices are provided. As the technology behind smart watches develops, so do the opportunities for security exploitation and malicious attacks.

Attention to addressing the known vulnerabilities has been steadily increasing with advancements to improve the security of smart watches proposed by researchers ranging from lightweight authentication methods to segregated trusted execution environments. In addition, government bodies are providing security codes of practices, pushing for new employment legislation, and military organizations banning the use of smart watches. These are all promising signs that can help remediate the risks and ensure a safe environment for the user.

Given the flaws highlighted by several studies, one would think either malicious attackers are yet fully committed to this technology with their focus on higher prized assets, or users have a level of security awareness to provide a layer of protection against the vulnerabilities. However, as with any IoT device, it is only a matter of time until the likes of sensitive information are exposed from eavesdropping on a government official, an organization dealing with a ransomware demand after exploiting a smart watch gave hackers the route into the company's network, or a large-scale data dump of pictures of children taken from smart watches is available on the dark web.

At a user level, retailers should be held more accountable for selling smart watches with known vulnerabilities, alongside clear advice provided to users on which devices are secure and preferred by industry-leading professionals. One approach could be applying a 'Security Score, 'like the energy consumption score listed on white appliances, that gives the user clear, straightforward information on the risks and privacy issues that a consortium of governing bodies has assessed. For example, an Apple Watch would score a high score based on is extra layers of encryption typically found within Apple devices. However, a low-end device would score low based on the ease for attackers to expose data and access key connection exchanges.

6. CONCLUSION

In conclusion, these findings suggest that the security of smart watches requires a greater level of understanding, and future research should concentrate on the methods to remediate highlighted risks. These findings imply that researchers in a controlled setting have investigated only a select number of smart watches to discover the security flaws. Additionally, the general lack of research into the user's privacy awareness, supporting legislation, and partnership with the industry proved to be a significant gap in the literature. Therefore, it is proposed that future research should be conducted in parallel with the manufacturers and government bodies to combine knowledge and promote a collaborative industry.

In addition, I recommend that smart watches should have mandatory security protection governed by a set of security regulations and policies that protect data privacy and exposure from potential attacks. Proper security concepts, controls, and mechanisms must be integrated before and during the design and architectural period to produce a secure product. Security issues should not be an after thought that causes oversights, increased costs, and less reliability for both the user and manufacturer[60]. Integrating security into the design of smart watches by increasing the computation power to handle stronger authentication and encryption methods has been highlighted to protect against malicious attacks. It is concerning that most connected systems are configured vulnerable by default, allowing malware to exploit technology and personal information[118]. Advancements in artificial intelligence, cognitive computing, deep learning, and the merging of the physical and digital worlds have created new security challenges to protect information alongside presenting the opportunity for alternative concepts to pioneer information security into a new era[119]. Smart watch functionality will continue to evolve into an environment where more sensitive data is tracked and shared amongst third parties such as healthcare providers and insurance companies while having the ability to control other IoT devices will become the norm.

Finally, a smart watch contains sensitive information. However, the categorization of this data under the legislation is vague and undefined. For example, GDPR does not distinguish between health and lifestyle data, with HIPAA protection not applying to re-engineered data and specific datasets. Technological advancements in transforming the smart watch from a GPS tracking device to a cutting-edge IoT wearable have brought significant benefits to the user, but these come at a cost from the extensive data tracking. Despite these developments, data protection laws have been slow in responding to the required legislation and standards to protect the user. However, on the other hand, security protection always starts with the user. In addition, the infrastructure of smart watches makes it challenging to use authentication protection, with low computation power and a lack of embedded security monitoring software. Therefore, should the smart watch manufacturers be held responsible for not providing basic security parameters outside of their privacy policies and online guides?

REFERENCES

[1] B. Carte and L. Miles. "The 12 best smartwatches for kids who don't need a smartphone just yet." https://www.bestproducts.com/tech/gadgets/g3115/best-smartwatch-for-kids/ (accessed 17 March, 2021).

[2] M. Rimol. "Gartner Forecasts Global Spending on Wearable Devices to Total $81.5 Billion in 2021." https://www.gartner.com/en/newsroom/press-releases/2021-01-11-gartner-forecasts-global-spending-on-wearable-devices-to-total-81-5-billion-in-2021 (accessed 17 March, 2021).

[3] J. Koetsier. "Global Smartwatch Market: Apple 34%, Huawei 8%, Samsung 8%, Fitbit 4.2%." https://www.forbes.com/sites/johnkoetsier/2021/05/27/global-smartwatch-market-apple-34-huawei-8-samsung-8-fitbit-42/ (accessed 28 May, 2021).

[4] C. Gartenberg. "Google's new Samsung smartwatch partnership looks a lot like giving up." https://www.theverge.com/2021/5/23/22448165/google-samsung-wearable-partnership-wear-os-tizen-merge-smartwatch (accessed 28 May, 2021).

[5] ResearchandMarkets. "Australia Wearables Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)." https://www.researchandmarkets.com/reports/5239653/australia-wearables-market-growth-trends (accessed 17 March, 2021).

[6] P. Lamkin. "Apple Still Leading The Way With Smartwatch Shipments But Huawei Is Hot On Its Heels." https://www.forbes.com/sites/paullamkin/2020/08/26/apple-still-leading-the-way-with-smartwatch-shipments-but-huawei-is-hot-on-its-heels/?sh=7de2866f169f (accessed 24 April, 2021).

[7] MordorIntelligence. "SMARTWATCH MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2021 - 2026)." https://www.mordorintelligence.com/industry-reports/smartwatch-market (accessed 29 April, 2021).

[8] S. Mete. "Wearable Spending to Hike Further: 4 Tech Stocks to Consider." https://www.nasdaq.com/articles/wearable-spending-to-hike-further%3A-4-tech-stocks-to-consider-2021-01-13 (accessed 17 March, 2021).

[9] Kaspersky. "Smartwatch Security - Safety & Risks." https://www.kaspersky.com.au/resource-center/threats/smartwatch-security-risks (accessed 18 March, 2021).

[10] Norton. "Smart watches and internet security: Are my wearables secure?" https://us.norton.com/internetsecurity-iot-how-to-protect-your-connected-wearables.html (accessed 18 March, 2021).

[11] J. Thompson. "A Concise History of the Smartwatch." https://www.bloomberg.com/news/articles/2018-01-08/a-concise-history-of-the-smartwatch (accessed 17 March, 2021).

[12] S. Lim. "Global Smartwatch Shipments Jump 35% YoY in Q1 2021." https://www.counterpointresearch.com/global-smartwatch-shipments-q1-2021/ (accessed 29 May, 2021).

[13] L. Goasduff. "Gartner Says Global End-User Spending on Wearable Devices to Total $52 Billion in 2020." https://www.gartner.com/en/newsroom/press-releases/2019-10-30-gartner-says-global-end-user-spending-on-wearable-dev (accessed 17 March, 2021).

[14] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, "A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server," *Computers & Electrical Engineering,* vol. 63, pp. 168-181, 2017.

[15] C. Saatjohann, F. Ising, L. Krings, and S. Schinzel, "STALK: security analysis of smartwatches for kids," in *ACM International Conference Proceeding Series,* ed: ACM, 2020, pp. 1-10.

[16] M. Williams, J. R. C. Nurse, and S. Creese, "Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study," *Computers in human behavior,* vol. 99, pp. 38-54, 2019, doi: 10.1016/j.chb.2019.04.026.

[17] P. Paganini. "Smartwatch Hacked, how to access data exchanged with Smartphone." http://securityaffairs.co/wordpress/31007/intelligence/smartwatch-hacked.html (accessed 07 May, 2021).

[18] E. S. Udoh and A. Alkharashi, "Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students," in *2016 Future Technologies Conference (FTC),* 2016: IEEE, pp. 926-931.

[19] J. Chokkattu. "CES 2021 Highlights: 79 Gadgets and Glimpses Into the Future." https://www.wired.com/story/ces-2021-highlights-liveblog-whole-show/ (accessed 29 May, 2021).

[20] D. Reisinger. "7 Must-Have Gadgets For Men Who Love Tech." https://www.forbes.com/sites/forbes-personal-shopper/2020/03/16/7-must-have-gadgets-for-men-who-love-tech/?sh=7c77a6931d86 (accessed 29 May, 2021).

[21] M. Guerar, M. Migliardi, F. Palmieri, L. Verderame, and A. Merlo, "Securing PIN-based authentication in smartwatches with just two gestures," *Concurrency and computation,* vol. 32, no. 18, p. n/a, 2020, doi: 10.1002/cpe.5549.

[22] A. Greenberg. "Kids' Smartwatches Are a Security Nightmare Despite Years of Warnings." https://www.wired.com/story/kid-smartwatch-security-vulnerabilities/ (accessed 23 April, 2021).

[23] C. Rouland. "Opinion: Beware that fake smartwatch. It's a malware magnet." https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0615/Opinion-Beware-that-fake-smartwatch.-It-s-a-malware-magnet (accessed 24 April, 2021).

[24] N. C. Council, "WatchOut: Analysis of Smartwatches for Children," *Norwegian Consumer Council Report,* 2017.

[25] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," *International journal of medical informatics (Shannon, Ireland),* vol. 88, pp. 8-17, 2016, doi: 10.1016/j.ijmedinf.2015.12.010.

[26] Y. Gao, H. Li, and Y. Luo, "An empirical study of wearable technology acceptance in healthcare," *Industrial management + data systems,* vol. 115, no. 9, pp. 1704-1723, 2015, doi: 10.1108/IMDS-03-2015-0087.

[27] H. Kang and E. H. Jung, "The smart wearables-privacy paradox: A cluster analysis of smartwatch users," *Behaviour & information technology,* pp. 1-14, 2020, doi: 10.1080/0144929X.2020.1778787.

[28] Apple. "System security for watchOS." https://support.apple.com/en-gb/guide/security/secc7d85209d/web (accessed 29 May, 2021).

[29] Samsung. "Set a Security Lock on your Samsung smart watch." https://www.samsung.com/us/support/answer/ANS00078771/ (accessed 29 May, 2021).

[30] Huawei. "HUAWEI WATCH FIT." https://consumer.huawei.com/en/support/wearables/watch-fit/ (accessed 29 May, 2021).

[31] S. Richardson and D. Mackinnon, "Left to their own devices? Privacy implications of wearable technology in Canadian workplaces," *Surveillance Studies Centre,* 2017.

[32] Statista. "Market share of smartwatch unit shipments worldwide from the 2Q'14 to 1Q '20*, by vendor." https://www.statista.com/statistics/524830/global-smartwatch-vendors-market-share/ (accessed 24 April, 2021).

[33] P. Ducklin. "Creepy covert camera "feature" found in popular smartwatch for kids." https://nakedsecurity.sophos.com/2020/10/13/creepy-covert-camera-feature-found-in-popular-smartwatch-for-kids/ (accessed 24 April, 2021).

[34] A. Henriksen *et al.*, "Using Fitness Trackers and Smartwatches to Measure Physical Activity in Research: Analysis of Consumer Wrist-Worn Wearables," *Journal of medical Internet research,* vol. 20, no. 3, pp. e110-e110, 2018, doi: 10.2196/jmir.9157.

[35] J. Allen, "Photoplethysmography and its application in clinical physiological measurement," *Physiological measurement,* vol. 28, no. 3, p. R1, 2007.

[36] P. A. Gloor, A. F. Colladon, F. Grippa, P. Budner, and J. Eirich, "Aristotle Said "Happiness is a State of Activity" — Predicting Mood Through Body Sensing with Smartwatches," *Journal of systems science and systems engineering,* vol. 27, no. 5, pp. 586-612, 2018, doi: 10.1007/s11518-018-5383-7.

[37] G. M. Weiss, K. Yoneda, and T. Hayajneh, "Smartphone and Smartwatch-Based Biometrics using Activities of Daily Living," *IEEE access,* vol. 7, pp. 1-1, 2019, doi: 10.1109/ACCESS.2019.2940729.

[38] J. Wan *et al.*, "Wearable IoT enabled real-time health monitoring system," *EURASIP journal on wireless communications and networking,* vol. 2018, no. 1, pp. 1-10, 2018, doi: 10.1186/s13638-018-1308-x.

[39] S. Kumar *et al.*, "A Wristwatch-Based Wireless Sensor Platform for IoT Health Monitoring Applications," *Sensors (Basel, Switzerland),* vol. 20, no. 6, p. 1675, 2020, doi: 10.3390/s20061675.

[40] C. E. King and M. Sarrafzadeh, "A survey of smartwatches in remote health monitoring," *Journal of healthcare informatics research,* vol. 2, no. 1, pp. 1-24, 2018.

[41] S. Ranger. "Driving stressed or sleepy? Soon your smartwatch will be able to warn your car." https://www.zdnet.com/article/driving-stressed-or-sleepy-soon-your-smartwatch-will-be-able-to-warn-your-car/ (accessed 29 April, 2021).

[42] F. Lambert. "Tesla is involved in the development of a smartwatch, but why?" https://electrek.co/2020/08/10/tesla-smartwatch-why/ (accessed 29 April, 2021).

[43] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in Bluetooth technology as used in IoT," *Journal of Sensor and Actuator Networks,* vol. 7, no. 3, p. 28, 2018.

[44] K. Sairam, N. Gunasekaran, and S. R. Redd, "Bluetooth in wireless communication," *IEEE Communications Magazine,* vol. 40, no. 6, pp. 90-96, 2002.

[45] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of Bluetooth security vulnerabilities," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, 2017: IEEE, pp. 1-7.

[46] S. Zeadally, F. Siddiqui, and Z. Baig, "25 years of bluetooth technology," *Future Internet,* vol. 11, no. 9, p. 194, 2019.

[47] K. Torvmark. "Three flavors of Bluetooth®: Which one to choose?" https://www.ti.com/lit/wp/swry007/swry007.pdf (accessed 29 May, 2021).

[48] D. De Cremer, B. Nguyen, and L. Simkin, "The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side," *Journal of marketing management,* vol. 33, no. 1-2, pp. 145-158, 2017, doi: 10.1080/0267257X.2016.1247517.

[49] S. Ranger. "Why your smartwatch and wearable devices are the next big privacy nightmare." https://www.zdnet.com/article/smartwatch-data-collection-rush-raises-privacy-backlash-fears/ (accessed 23 April, 2021).

[50] M. Taylor, D. Reilly, and C. Wren, "Internet of things support for marketing activities," *Journal of strategic marketing,* vol. 28, no. 2, pp. 149-160, 2020, doi: 10.1080/0965254X.2018.1493523.

[51] G. D. Vynck and L. Baker. "Google's Fitbit deal under fire amid competition and privacy concerns." https://www.afr.com/technology/google-s-fitbit-deal-under-fire-amid-competition-and-privacy-concerns-20191103-p536y3 (accessed 23 April, 2021).

[52] J. Bursztynsky. "Google closes its Fitbit acquisition." https://www.cnbc.com/2021/01/14/google-closes-its-fitbit-acquisition.html (accessed 23 April, 2021).

[53] Kaspersky. "Smartwatch Security - Safety & Risks." https://www.kaspersky.com.au/resource-center/threats/smartwatch-security-risks (accessed 29 May, 2021).

[54] N. Goud. "Cyber Attacks on fitness trackers, smartphones, and voice-activated gadgets." https://www.cybersecurity-insiders.com/cyber-attacks-on-fitness-trackers-smartphones-and-voice-activated-gadgets/ (accessed 17 March, 2021).

[55] J. Porter. "Garmin reportedly paid multimillion-dollar ransom after suffering cyberattack." https://www.theverge.com/2020/8/4/21353842/garmin-ransomware-attack-wearables-wastedlocker-evil-corp (accessed 21 March, 2021).

[56] A. Uribe. "Medical data more valuable than credit card details on the dark web." https://www.afr.com/companies/financial-services/medical-data-more-valuable-than-credit-card-details-on-the-dark-web-20170707-gx6na4 (accessed 18 April, 2021).

[57] M. Leonhardt. "Here's how much money hackers get for your Social Security Number and other info on the black market " https://www.cnbc.com/2018/08/22/how-much-hackers-get-for-social-security-numbers-on-the-black-market.html (accessed 18 April, 2021).

[58] V. Kumar, D. Ramachandran, and B. Kumar, "Influence of new-age technologies on marketing: A research agenda," *Journal of business research,* vol. 125, pp. 864-877, 2021, doi: 10.1016/j.jbusres.2020.01.007.

[59] N. Gerhart and O. Ogbanufe, "Disidentity and nonconsumption of smartwatches," *International journal of consumer studies,* 2021, doi: 10.1111/ijcs.12666.

[60] M. Chapple, J. M. Stewart, and D. Gibson, *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*. John Wiley & Sons, 2018.

[61] S. J. Tipton, S. Forkey, and Y. B. Choi, "Toward proper authentication methods in electronic medical record access compliant to HIPAA and CIA triangle," *Journal of medical systems,* vol. 40, no. 4, p. 100, 2016.

[62] T. K. Buennemeyer, "A strategic approach to network defense: framing the cloud," ARMY WAR COLL CARLISLE BARRACKS PA, 2011.

[63] A. Henderson. "The CIA Triad: Confidentiality, Integrity, Availability." http://panmore.com/the-cia-triad-confidentiality-integrity-availability (accessed 18 April, 2020).

[64] K. Crawley. "All About the CIA Triad." https://threatvector.cylance.com/en_us/home/all-about-the-cia-triad.html (accessed 13 April, 2021).

[65] Q. Do, B. Martini, and K. K. R. Choo, "Is the data on your wearable device secure? An Android Wear smartwatch case study," *Software: Practice and Experience,* vol. 47, no. 3, pp. 391-403, 2017.

[66] D. Walkowski. "What is the CIA Triad?" https://www.f5.com/labs/articles/education/what-is-the-cia-triad (accessed 10 April, 2021).

[67] A. K. Das, S. Zeadally, and M. Wazid, "Lightweight authentication protocols for wearable devices," *Computers & Electrical Engineering,* vol. 63, pp. 196-208, 2017.

[68] W. Liu, H. Liu, Y. Wan, H. Kong, and H. Ning, "The yoking-proof-based authentication protocol for cloud-assisted wearable devices," *Personal and Ubiquitous Computing,* vol. 20, no. 3, pp. 469-479, 2016.

[69] N. B.-N. I. Minar and M. Tarique, "Bluetooth security threats and solutions: a survey," *International Journal of Distributed and Parallel Systems,* vol. 3, no. 1, p. 127, 2012.

[70] T. Panse and P. Panse, "A survey on security threats and vulnerability attacks on bluetooth communication," *International Journal of Computer Science and Information Technologies,* vol. 4, no. 5, pp. 741-746, 2013.

[71] B. L. Parne, S. Gupta, and N. S. Chaudhari, "ESAP: Efficient and secure authentication protocol for roaming user in mobile communication networks," *Sadhana (Bangalore),* vol. 43, no. 6, pp. 1-19, 2018, doi: 10.1007/s12046-018-0879-x.

[72] S. Liu, S. Hu, J. Weng, S. Zhu, and Z. Chen, "A novel asymmetric three-party based authentication scheme in wearable devices environment," *Journal of Network and Computer Applications,* vol. 60, pp. 144-154, 2016.

[73] Z. Wang, C. Shen, and Y. Chen, "Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics," ed. Cham: Springer International Publishing, 2017, pp. 545-553.

[74] M. Gault. "The CIA Secret to Cybersecurity That No One Seems to Get." https://www.wired.com/2015/12/the-cia-secret-to-cybersecurity-that-no-one-seems-to-get/ (accessed 14 April, 2021).

[75] M. E. Gladden, "An Axiology of Information Security for Futuristic Neuroprostheses: Upholding Human Values in the Context of Technological Posthumanization," *Frontiers in neuroscience,* vol. 11, p. 605, 2017.

[76] J. P. L. Goh, "Privacy, security, and wearable technology," *Landslide (Chicago, Ill.),* vol. 8, no. 2, p. 30, 2015.

[77] V. Stykas. "Hacking smart devices to convince dementia sufferers to overdose." https://www.pentestpartners.com/security-blog/hacking-smart-devices-to-convince-dementia-sufferers-to-overdose/ (accessed 24 April, 2021).

[78] A. Atamli-Reineh, A. Paverd, G. Petracca, and A. Martin, "A framework for application partitioning using trusted execution environments," *Concurrency and computation,* vol. 29, no. 23, pp. e4130-n/a, 2017, doi: 10.1002/cpe.4130.

[79] S. Samonas and D. Coss, "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY," *Journal of Information System Security,* vol. 10, no. 3, 2014.

[80] P. Lamkin. "Smartwatch timeline: The devices that paved the way for the Apple Watch." https://www.wareable.com/smartwatches/smartwatch-timeline-history-watches (accessed 21 March, 2021).

[81] K. Purdy. "Should You Get a GPS Running Watch, Fitness Tracker, or Smartwatch?" https://www.nytimes.com/wirecutter/blog/gps-running-watch-fitness-tracker-or-smartwatch/ (accessed 21 March, 2021).

[82] L. Piwek, D. A. Ellis, S. Andrews, and A. Joinson, "The Rise of Consumer Health Wearables: Promises and Barriers," *PLoS medicine,* vol. 13, no. 2, pp. e1001953-e1001953, 2016, doi: 10.1371/journal.pmed.1001953.

[83] M. Sweney. "Smartwatch maker Garmin hit by outages after ransomware attack." https://www.theguardian.com/business/2020/jul/24/smartwatch-maker-garmin-hit-by-outages-after-ransomware-attack (accessed 29 May, 2021).

[84] M. Mahinderjit Singh, K. W. Ching, and A. Abd Manaf, "A novel out-of-band biometrics authentication scheme for wearable devices," *International journal of computers & applications,* vol. 42, no. 6, pp. 589-601, 2020, doi: 10.1080/1206212X.2018.1547347.

[85] J. Davis. "Data of 43,000 patients breached after theft of unencrypted laptop." https://www.healthcareitnews.com/news/data-43000-patients-breached-after-theft-unencrypted-laptop (accessed 29 May, 2021).

[86] R. Norton-Taylor. "Lost MI6 laptop contained training notes for agents." https://www.theguardian.com/uk/2000/mar/29/richardnortontaylor (accessed 29 May, 2021).

[87] D. C. Klonoff, "Cybersecurity for Connected Diabetes Devices," *Journal of diabetes science and technology,* vol. 9, no. 5, pp. 1143-1147, 2015, doi: 10.1177/1932296815583334.

[88] J. Soni. "Locating a lost Galaxy Smartwatch might get difficult - here's why." https://www.techradar.com/news/locating-a-lost-galaxy-smartwatch-might-get-difficult-heres-why (accessed 29 May, 2021).

[89] T. Burton. "Internet of things sets the cat among the pigeons." https://www.afr.com/technology/internet-of-things-sets-the-cat-among-the-pigeons-20201001-p5612g (accessed 21 March, 2021).

[90] ACSC, "IoT Code of Practice: Guidance for Manufacturers." [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-09/PROTECT%20-%20IoT%20Code%20of%20Practice%20%E2%80%93%20Guidance%20for%20Manufacturers%20%28September%202020%29.pdf

[91] A. Chanthadavong. "Australian government releases voluntary IoT cybersecurity code of practice." https://www.zdnet.com/article/australian-government-releases-voluntary-iot-cybersecurity-code-of-practice/ (accessed 30 May, 2021).

[92] V. Kumari and S. A. Hook, "The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly?," ed. Cham: Springer International Publishing, 2017, pp. 50-64.

[93] A. Williams. "Google Now Owns Fitbit: What It Means For Your Fitness Data Privacy." https://www.forbes.com/sites/andrewwilliams/2021/01/14/google-now-owns-fitbit-what-it-means-for-your-fitness-data-privacy/?sh=708ad91539e1 (accessed 19 March, 2021).

[94] E. A. Brown, "The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work," *Yale journal of health policy, law, and ethics,* vol. 16, no. 1, pp. 1-49, 2016.

[95] P. M. Schwartz and D. J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information," *NYUL rev.,* vol. 86, p. 1814, 2011.

[96] P. Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA l. Rev.,* vol. 57, p. 1701, 2009.

[97] L. Sweeney, J. S. Yoo, L. Perovich, K. E. Boronow, P. Brown, and J. G. Brody, "Re-identification Risks in HIPAA Safe Harbor Data: A study of data from one environmental health study," *Technology science,* vol. 2017, 2017.

[98] T. Sullivan. "General Wellness: Policy for Low Risk Devices Draft Guidance for Industry and Food and Drug Administration Staff." https://www.policymed.com/2015/01/fda-device-guidance-general-wellness-policy-for-low-risk-devices.html (accessed 18 April, 2021).

[99] N. Wetsman. "Fitbit’s Sense smartwatch gets FDA clearance for EKG app." https://www.theverge.com/2020/9/14/21436090/fitbit-sense-ekg-heart-fda-clearance-apple-samsung-withings (accessed 29 May, 2021).

[100] N. R. Odom, J. M. Lindmar, J. Hirt, and J. Brunty, "Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices," *Journal of forensic sciences,* vol. 64, no. 6, pp. 1673-1686, 2019.

[101] R. Opie. "Smartwatch data helped police make arrest in Adelaide murder case, court hears." https://www.abc.net.au/news/2018-03-29/smart-watch-data-helps-police-find-suspect-in-murder-case-court/9602832 (accessed 30 May, 2021).

[102] R. Becker *et al.*, "DAISY: A Data Information System for accountability under the General Data Protection Regulation," *Gigascience,* vol. 8, no. 12, 2019, doi: 10.1093/gigascience/giz140.

[103] S. Charara and H. Sumra. "We read your wearable tech's privacy policy so you don't have to." https://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765 (accessed 30 May, 2021).

[104] S. Wachter, "The GDPR and the Internet of Things: a three-step transparency model," *Law, innovation and technology,* vol. 10, no. 2, pp. 266-294, 2018, doi: 10.1080/17579961.2018.1527479.

[105] GDPR. "Processing of special categories of personal data." https://gdpr-info.eu/art-9-gdpr/ (accessed 30 May, 2021).

[106] D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, "Disruptive and avoidable: GDPR challenges to secondary research uses of data," *European journal of human genetics : EJHG,* vol. 28, no. 6, pp. 697-705, 2020, doi: 10.1038/s41431-020-0596-x.

[107] V. Ioannidou. "European Union: The GDPR And The Effect On The Medical Profession." https://www.mondaq.com/cyprus/data-protection/861664/the-gdpr-and-the-effect-on-the-medical-profession (accessed 30 May, 2021).

[108] C. B. Olsen, "To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR," *International data privacy law,* vol. 10, no. 3, pp. 236-252, 2020, doi: 10.1093/idpl/ipaa004.

[109] J.-L. Gómez-Barroso, C. Feijóo, and I. J. Martínez-Martínez, "Privacy calculus: Factors that influence the perception of benefit," *El profesional de la información (EPI),* vol. 27, no. 2, pp. 341-348, 2018.

[110] S. Pike, M. Kelledy, and A. Gelnaw, "Measuring US privacy sentiment: An IDC special report," in *Technical Report,* 2017.

[111] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of consumer affairs,* vol. 41, no. 1, pp. 100-126, 2007.

[112] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, "User evaluation of lightweight user authentication with a single tri-axis accelerometer," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services,* 2009, pp. 1-10.

[113] T. V. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," *Computers & security,* vol. 66, pp. 115-128, 2017, doi: 10.1016/j.cose.2017.01.008.

[114] J. Hahn. "China's army banned smartwatches." https://www.businessinsider.com/chinas-army-banned-smartwatches-2015-5?IR=T (accessed 29 April, 2021).

[115] N. Goud. "Smart Watches used by teenagers are vulnerable to Cyber Attacks." https://www.cybersecurity-insiders.com/smart-watches-used-by-teenagers-are-vulnerable-to-cyber-attacks/ (accessed 29 April, 2021).

[116] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," *arXiv preprint arXiv:1901.02672,* 2019.

[117] S. A. Razak, "Aiming for Cyber Safety," *ITNow,* vol. 58, no. 4, pp. 34-35, 2016, doi: 10.1093/itnow/bww104.

[118] S. Furnell and E. H. Spafford, "The Morris Worm at 30," *ITNOW,* vol. 61, no. 1, pp. 32-33, 2019.

[119] L. Shave, "The CIA of security and access," *IQ: The RIM Quarterly,* vol. 34, no. 2, p. 18, 2018.