Subcutaneous Body Area Networks - A SWOT Analysis

2015 IEEE International Symposium on Technology in Society (ISTAS) Proceedings
ISBN: 978-1-4799-8283-7

Subcutaneous Body Area Networks

A SWOT analysis

P. A. Catherwood, D.D. Finlay, J.A.D. McLaughlin
School of Engineering, Ulster University, Jordanstown, N. Ireland.
Email: p.catherwood@ulster.ac.uk

***Abstract*—This paper presents a SWOT analysis for the emerging and futuristic field of non-medical body-implantable devices. This area will begin to materialize as one of the next big themes in future personal computing and offers huge rewards to society if implemented correctly. The technology boasts many strengths which are applicable to a variety markets including entertainment, social networking, personal safety, security, consumerism, communications, healthcare, convenience and human body enhancement. Such subcutaneous sensor technology releases citizens from the multitude of portable computing devices, keys, wallets, passes, etc. However, the technology would be a target for hackers and would likely result in more violent robberies and forceful ID removal. Additionally, adverse health effects, device and battery safety and reliability, and co-existence with medically prescribed implants are issues developers must solve before the technology could excel. External emerging technologies such as Cloud computing, IoT, and NFC support development and potential success of implantable systems and combines to help address issues of personal safety, terrorism, people tracking and identification, e-payments, and long-term fitness profiling. Threats to the technology's uptake include societal fears on such aspects as adverse health effects, dehumanisation, breaches of human rights, conservatism, social privacy, and religious objections. With this technology potentially beginning to enter the mainstream in the next 5-10 years considerable effort is required to develop legislation, policies, procedures, device and network security, and convince the general public this technology is the next logical step in personal computing.**

Keywords—Body area network; consumer electronics; implants; in-body; IoT; NFC; on-body; RFID; sensors; subcutaneous; SWOT; wearables; wireless.

I. INTRODUCTION

There exists long history of implantable devices for medical purposes; examples include pace makers [1], cochlear and retinal implants [2], insulin pumps [3], deep brain stimulation implants for relief of Parkinson's disease tremors and seizures [4, 5], to name but a few. These are specifically implantable medically-prescribed devices to assist the treatment of chronic health conditions.

As the emerging Internet of Things (IoT) develops there is a growing trend towards wearable consumer electronics for a myriad of applications, including interactive haptic environments [6], healthcare [7], high data rate communications systems [8], wearable interfaces [9], people tracking [10], etc. The two domains of implantable medical devices and wearable consumer electronics overlap in the incipient world of subcutaneous consumer electronics devices. Such devices are not categorized as medical devices designed for sustaining life or for improving the quality of life of those with chronic conditions. Instead they are a range of networked biocompatible consumer electronics devices that users will choose to have implanted into their body to take advantage of new technologies for purposes of convenience, communication, entertainment, shopping, and security. To date body-implantable electronic devices have been the remit of research centers and fringe enthusiast groups [11], but it is envisaged that such technology will enter the mainstream in the nearing future [12], with the vision being one of ubiquitous connectivity – an Internet of Everything (IoE), including humans [13].

This paper presents a SWOT analysis (strengths, weaknesses, opportunities, and threats) for the field of emerging and futuristic non-medical body-implantable devices with the purpose of identifying, understanding, and evaluating the strategic factors which assist or hinder mainstream realisation, and the internal/external forces with which the technology is confronted. Such an analysis is essential for strategic technology planning and inherently considers factors and forces from the aspect of the technology and the users adopting them. The paper also discusses current and emerging trends and technologies, and analyses predicted future technologies that will usher in this new era of human-technology interaction. This article aims to emphasize the profile of both the fledgling technology and its assortment of hurdles. Such complications must receive timely address by legislators and engineers to ensure the technology is both successful and safe before systems develop a commercial presence.

II. CURRENT AND EMERGING TRENDS

A. Social Trends

There exists a new generation of makers, hackers, and early-adopters; with this comes increasing acceptance of technological possibilities that the previous generation as a whole would have shunned without consideration. Younger members of society document their lives on the internet for anyone to browse and comment upon, with seemingly scarce

regard for security or privacy at times. These individuals typically spend a sizable portion of their personal wealth on popular consumer electronics, including smartphones, tablets, smartwatches, novelty apps. and gadgets, etc.

There is also a rising social trend of tattooing and body piercing with approximately 10% of those surveyed in England in 2005 having body piercings in places other than the earlobe [14], one in seven Australian adults report having a tattoo [15], and the percentage of tattooed adults in the US rising from 14% in 2008 to 21% in 2012 [16]. This trend is significant as it highlights potential acceptance of subcutaneous objects, skin e-tattoos, etc. Tattoos, piercings and implants are all definable as deliberate alterations of the human body and most bio-hackers (fringe groups who self-mutilate and insert various electronic and non-electronic objects on, in, and under the skin) also have multiple tattoos and piercings [17, 18].

B. Technology Trends

Technology continues to get smaller, smarter, and more powerful in both processing and data mining terms. Current medical knowledge also understands the body much better than at any time in the past and continues to expand its comprehension of both cell and organ interactions with modern materials and technologies [19]. Biocompatibility has become of key interest in developing dental implants, joint replacement, bone cement, skin scaffolding, encapsulation methods for implanted devices, etc. [20]. Medical implants are defined as those implants that are prescribed and fitted by medical practitioners for the purpose of replacing missing biological structure, sustaining life and/or alleviating the symptoms of chronic illness. The best known electronic medical implant is the aforementioned cardiac pace maker, although various mechanical implants such as stints, hip joints, pins and plates, and birth control devices are also very much common place today.

This paper focuses on those other devices that are not medically prescribed. Instead, these non-medical implants will typically be devices that are selected by a user in the same way that portable consumer electronics are currently chosen, the key difference being their subcutaneous nature. A number of consumer implantable electronic devices already exist, such as the personal identity Verichip (now PositiveID) [21], and rarely a day passes without new smart wearable or future embedded devices making headlines. Such examples include various body-electrodes that create a brain-computer interface (BCI) to operate machines using thought [22, 23], stretchable on-body touch and sensors electronic skin tattoos for mobile computing [24, 25], wearable technologies that utilize bodies as fuel sources [26], contact lenses with controllable magnification using winking [27], and disability-eliminating cyborg systems [28], to name a few.

Cloud computing and the IoT are emerging technologies that will enable early generations of implanted body networks. The current wearables market is an indicator for the future implantables market, and the fast developing wearables market already has a multitude of support industries growing around it which provide technology and services (customisation, repair, etc.). It is possible to categorize these implants into subgroups such as entertainment, healthcare, security/safety, and financial, although all would go under the banner of consumer electronics devices.

There are a number of target areas for implantable technologies, some of which are presented in Figure 1. Target areas include automatic gesture control, haptic sensors, and movement detection implants for device control in the home, work, car, gaming, etc. which offer higher levels of integration, interaction and enjoyment for the user. Other implants would include aural/retinal implants to recover lost hearing/vision or enhance natural senses, and also for embedded communications devices. An embedded microphone and camera technology would complement these with the potential to replace portable smartphones.

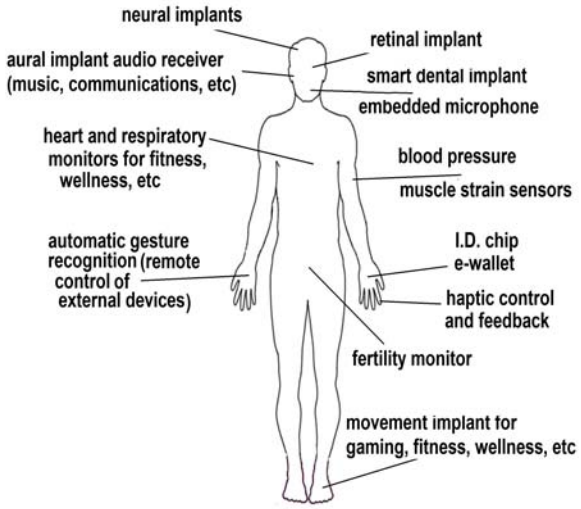

Fig. 1. Target areas for implantable body-area network technologies

E-wallet chips would enable secure purchases without cash, offering management of daily spending limits, etc. while neural implants allow control of every external device in an individual's personal IoE without the requirement to press a single button. Other examples include dental implants to monitor oral health, eating patterns, dietary intake, etc., muscle strain sensors to reduce the risk of muscular injury and highlight the level of fitness workouts, fertility monitors to assist with family planning or abstinence monitoring, internal health monitors to detect illnesses before they develop too far (e.g. bowel cancer) and blood pressure sensors to keep a real-time eye on the "silent killer" [29]. The last few overlap strongly with medical implantable devices, but many of these sensors may be personal options instead of medically prescribed solutions.

This aforementioned technology is a subset of a larger classification which sees the convergence of consumer technology, robotics, genetics, nanotechnology and artificial intelligence. Such synergies could potentially realize networked bio-technology systems that offer significantly superior intelligence and functionality to the host human; while this is many years away it does suggest the potential in the emerging capabilities of the combined industries.

III. S.W.O.T. ANALYSIS

A SWOT analysis is a powerful exploration device that studies the strengths, weaknesses, opportunities, and threats to analyze the internal and external influencing factors that determine the potential success of a particular technology,

business model or corporate strategy. The strengths and weaknesses relate to matters internal to the technology and can be changed through technology revision and tactical R&D; the opportunities and threats are external to the technology, such as public opinion or political/financial climate, and can't easily be changed. Here the SWOT framework is being utilized for emerging and futuristic non-medical body-implantable systems and devices to outline key personal and societal benefits, and to understand the hurdles and opposition it faces in this current age.

It is recognized that a number of the points raised below are not necessarily unique to subcutaneous devices, and many ICT and personal computing devices which boast benefits of portability, efficiency and entertainment value also have issues regarding privacy, personal safety and hacking. However, embedding such technology into human bodies adds numerous new dimensions to the discussion.

A. Technology Strengths

Human-implantable sensor networks exhibit many tangible strengths. There already exists a suitable IEEE standard (IEEE.802.15.6-2012) to which engineers can base development upon [12]. The technology also directly targets multiple markets including entertainment, social networking, personal safety, security, consumerism, communications, healthcare, convenience, and in the future upgrading of human bodies to perform beyond their natural limitations. The technology can enhance future entertainment markets through such aspects as high data-rate streaming, networking with multiple users, environmental emersion and haptic-rich virtual reality environments for the user.

The technology lends itself to a new era in social networking activities and consumerism, the latter possibly employing implanted personal secure e-wallet as the next logical step after smartphone wallets [30]. Such e-transactions would help eliminate activities of ticket touting, financial transaction fraud, and robbery.

Indeed, personal safety is a fundamental reason to adopt implanted body-area networks as the technology could track location, and the sousveillence aspect of the technology would record personal interactions with others. (Sousveillence is monitoring by way of small portable wearable personal technologies [31]). It would add new levels of security through unique authentication for access to buildings and computers, removing the need for keys and passwords [32]. It would also reduce the number of kidnappings and volume of human trafficking as many individuals would have ID tracking implants.

One of the key aspects of this new technology would be in the area of personal electronic communications. The technology could replace mobile phones and other portable computing devices, with screens replaced with heads-up displays via glasses or contact lenses [33], keyboards on the skin [34], embedded or tattooed microphones [18], surfing the web using only thought [35], etc. This communications system would also wirelessly and seamlessly network with external wearable and personal devices.

Another fundamental strength is in the area of healthcare and wellbeing. While a distinct area of implantable medical devices is already established these are specifically to treat particular illnesses that cannot be efficiently and effectively be addressed by other means. Instead the current growing trend for wearable health and fitness monitors to measure and profile athletic performance signifies future market opportunities for implantables. For example, implanted dental sensors can monitor mouth pH levels, bruxism, and dietary habits at all times without intrusion.

The emerging technology of the Internet of Things and Internet of Everything opens up true opportunities for implanted body networks to realize a whole new realm of convenience through the automation of everything. Neural implants, gesture sensors, haptic sensors, eye gaze sensors, etc. offer real-time remote control of various objects, systems, and devices with a glance, a wave or a thought. Likewise, belongings such as cars and firearms could be personalized with NFC actuator chips controlling access and operation.

Ultimately these implanted networks could enhance the human body to what could accurately be described as super-human ability. Super vision and hearing, taste, feel and smell, an ability to sense movement outside of the field of view, x-ray vision, night vision, mind control of the local environment, artificial intelligence, and mind-reading through sensor-facilitated telepathy are all possibilities.

B. Technology Weaknesses

While the technology boasts authentication security, it is by its wireless nature a target for criminal activity including data profiling for nefarious purposes as aware users go about their daily business [36]. Likewise, while the technology can reduce robberies, those that do occur are more likely to be violent as the victims must make transactions in person. Furthermore, kidnappings and human trafficking will require forceful removal of ID and/or tracking implants.

Because these sensor networks are inserted into the human body there are questions over their safety, and many questions need to be addressed before general acceptance of the technology can be envisaged. Firstly, there is a basic requirement for devices to be implanted correctly in a way that does not cause damage to the body (e.g. muscles, nerves, and sinew). Also, there are questions regarding the long term health effects due to electromagnetic radiation from multiple devices, and for individual's bodies rejecting implants. Much like the breast enhancement problems with leaking implants [37], if there are adverse effects will the local healthcare system pay to rectify individual's personal lifestyle choices by removing the implants and treating any damage they caused?

Assuming subcutaneous medical device proliferation precedes non-medical devices there is a concern over interference with existing implanted medical devices. The implants acquired in ones 20s and 30s may interfere with the, then commonplace, medical implants in later life. There will hopefully be legislation and safeguards to ensure this is not the case, with interoperability of all devices the ideal scenario and non-interference the acceptable alternative. However, there will always be individuals and groups of individuals who do not use approved implants, or make and insert their own home-made technology [18]; the maker culture and 3D printing already make this a possibility now!

As with all technology, device reliability is an issue. More so if the device is embedded, as if it fails it must be extracted. Similarly, questions as to how the latest hardware upgrades are realized are highly valid. If batteries are used (most likely

in conjunction with energy-harvesting strategies) will there be long-term battery issues? Would such energy cells leak after a serious personal injury? Currently, chip life is expected to be around 10 years [32], which is not entirely acceptable considering their intended purpose.

Other issues such as how the technology should be implemented and rolled out are of concern. For example, a lack of strategic planning and a proliferation of homebrew makers could actually make things worse as devices created by amateur developers and start-ups may not synergistically work within the system as expected and required. Devices may be subject to software viruses, with potentially lethal consequences. Also, in very crowded environments where multiple users may physically touch each other (e.g. concerts) will devices interfere or share connectivity they should not? Security settings would address this but experience shows users are poor at ensuring their networked devices are suitably protected [38]. At the time of writing there also exists a lack of research into multipoint implanted BSNs, although this may not be the case as such systems approach realisation.

C. Technology Opportunities

Current and developing external factors give human-implantable devices a number of opportunities. There exists an emerging technology-obsessed generation who spend their expendable finances on the latest technology trends such as smartphones, headphones, gaming consoles, etc. Many upgrade to the next generation of a device while the previous is perfectly adequate for all their needs. Technology is as much an identity and fashion statement as it is a functional commodity. An indicator of this is the vibrant industry for smartphone and tablet customization (personalized covers, charms, ringtones, etc.). This rise in personal expression of the individual through technology and fashion is also observed through the increase in the number of people choosing tattoos, body piercings and other body art. Implanted networks would bring new levels of efficiency for everyday life including rapid procurement of goods via implanted e-wallet payments and ticketless verification of season passes. It would also eliminate lost money and tickets, and control access to buildings, vehicles, and computers.

Other contemporary social issues could be partially addressed by this technology. Examples include personal safety, terrorism, personal ID, tracking of missing persons, etc. Freedom from keys, cash, passports, ID documents, and cards is an attractive proposition that offers a futuristic feel. Already we are seeing laptops and phones with biometric scanners and guns that recognize their user [38]. Implanted personal computing removes the need to carry so many portable gadgets and thus would reduce the chance of street muggings and pick-pocketing as there is little to physically steal. It is also understood that embedded camera and sound recording technology would further add to this, as sousveillence typically reduces extortion [39].

Ubiquitous computing and sensing would be an effective way to reduce terrorist activities and perhaps reduce the impact of successful attacks by aiding recovery and identification of missing persons during disaster scenarios. The same is also true for natural disasters, transport disasters, etc. On the topic of personal ID, simple implanted tags are useful for the easy identification of lost individuals, such as children or the elderly. Similarly, the ability to remotely set financial limits for children's spending, accurate age confirmation for purchase of controlled substances and commercial goods, etc. are good reasons to purchase systems.

Additionally, the health benefits of having various implanted sensors in the body which monitor everything from internal body temperature, weight, toxin levels, etc. will help the adoption of the technology. Medicinal requirements of individuals can be easily and rapidly checked, for example if an individual went into a diabetic coma then those assisting could be made aware of the individual's medical needs. In a society both obsessed with wellness and immersed in unhealthy lifestyles, a system that is non-invasive to activities of daily living would be warmly received. Having sensors permanently monitoring your wellness as opposed to the "snap-shot" health sample at a treatment room would logically result in faster responses to developing conditions and more accurate diagnosis for emergency medical treatment. Furthermore, the opportunity to enjoy upgraded bodily senses (hearing, sight, etc.) is attractive and would make subcutaneous technology a valued commodity.

Implantable systems would offer genuine personalized experiences for entertainment, education, social networking and travel. A new generation of lifeloggers could use their personal network to record what they saw, heard and smelled, and also how they felt using physiological sensors.

Technologies such as cloud computing, big data, 5G+, smart cities, biocompatible materials, etc. all converge to assist the successful deployment and development of subcutaneous body area networks, ensuring they are usable, useful, networked, and safe. From the materials viewpoint, out of the thousands of metal alloys available very few can safely be used in the body. Usable biomaterials include stainless steel, alloys based on the cobalt chromium system, selected titanium alloys and the shape memory alloy of nickel and aluminum, [40, 41].

The concept of a super soldier has been discussed for some time, but in the near future this could be a reality. Implanted technologies could enhance a small group of special-force combatants with military functionality beyond what is naturally possible using a blend of neuroscience, biotechnology, robotics, etc. [42].

Perhaps the most extreme example of how implantable technology could be embraced comes from the small but growing Transhumanist movement who wish to enhance and repair their bodies indefinitely using advanced technology. These groups see technology not as just a solution to avoid illness and aid wellness, but as a vehicle to upgrade humans to superhuman semi-cyborg status [11]. Such groups have held conferences around the globe to share their vision and have attracted the attention of such organisations as California Technology Institute and Harvard University. Their goals include expanding human capabilities through technology and seek human-technology hybrids. While many will view such aspirations as nothing more than far-fetched scientific fiction, the desire in the modern era to have technology-enhanced bodies is clear.

The above opportunities highlight the potentially large long term market to satisfy consumer demand and the lucrative business opportunities for I.T. industries. Coupled with the increasing acceptance of tattoos and body piercings there is an emerging technology of flexible skin e-tattoos [43],

stretchable electronics [44] and ink-printable skin antennas [45] that all feed in to this brave new world.

D. Technology Threats

With the many opportunities come many threats. In fact, this embryonic technology suffers from more threats than most. Key threats revolve around society fears regarding technological, social, cultural, health, financial, security, crime, religious objection, and philosophical issues.

Even with the new wave of experimenters and hackers, society as a whole is still quite conservative and this could lead to a lack of adoption of the technology. A 2010 survey of individuals attending a technology conference conducted by BITKOM (a German information technology industry lobby group) reported 23% of 1000 respondents would be prepared to have a chip inserted under their skin for certain benefits; 72% of respondents, however, reported they would not allow implantation of a chip under any circumstances [46]. A trial conducted in 2010 in the Baja beach club in Barcelona, Spain offered club members implanted RFID chips which allowed them to make e-payments for bar refreshments and gave access to VIP areas. Despite the obvious benefits afforded to members the trial highlighted the lukewarm reception towards the technology [47].

Another major societal threat to implementation exists due to ingrained fears in society of being chipped and enslaved, with every movement tracked and every decision recorded, and also with identity theft based on the lack of security in current technology. Such problems include concerns over what data these systems are recording, how secure are they from hackers, where the data is being stored, what the data is being used for and by whom. All of these are very valid concerns and society will look to engineers, programmers, and legislators to bring robust transparent solutions. [48] highlights the fear that having an implantable computing device has a dehumanising effect, being effectively branded like cattle. This subcutaneous consumer electronics technology obviously has a much wider range of applications than mere identification using a chip, but it is the idea of civilized society being reduced to labelling everyone with an identifying number or code which is fundamentally repellent to some. Of course, the astute reader will note that this is already the case, examples being the social security and national insurance numbers in the US and UK respectively.

Fears over the protection of individual human rights and the perceived endless negative function creep (like GPS on phones being used to track users, web browsers tracking shopping habits, etc.) are threats to the technology as there is a growing backlash within communities of technology users who object to having their data mined by companies for marketing purposes [49]. Such fears reflect a wider trend of increasing distrust of businesses, governments and organisations which is fuelled by publicized high-profile leaks of data abuse such as tapping by the FDA, and the ability to track anyone anywhere in the world from a personal mobile signal as in the case of the global hunt for terrorists. Companies may use sensor proximity in public places to data-mine preferences, etc. and use this information to bombard individuals with personalized advertising, as is currently commonplace on the internet with constant consumer pop-ups and adverts. Employers may begin to utilize bodily sensor networks to facilitate employee monitoring, benchmarking and performance relate benefits [50].

Likewise, other people's implanted and wearable networks may infringe upon the rights of others in close proximity. The activity of lifelogging using embedded cameras is a growing trend amongst the young, with lifelogging cameras (such as Google Glass) recording everything that the user sees and does [51]. However, many object to being recorded by other people's devices [52]. In fact, such objections have already been realized in 2012 when Steve Mann, considered the father of wearable devices, was attacked in a French fast-food restaurant when an employee took exception to Mann wearing video-capture eyeglasses [53].

Other barriers to widespread implementation include a strong wearables market negating the attraction of implantables, and inadequate corporate funding to develop and propagate the technology. To ensure devices are not a health or technology hazard they will need reputable companies developing them, but for this to happen these companies need to foresee a return on their investment. If this return comes from advertisements, data collection or a monopoly on implantable systems then potential users may reject the technology or turn to cottage industry developers, which again raises safety concerns. Indeed, there already exist a number of fringe groups called "biohackers" or "grinders" who self-mutilate and implant all sorts of electronic and non-electronic items under their skin [18, 54], and also fanatical tattooists/piercers calling themselves 'flesh engineers' who provide implantation services [55], often with few safeguards.

Indeed, further hurdles include the fears due to unknown health risks of long term body implants, regardless of the quality of the devices. No data exists currently to evaluate the risks related to the use of long term bodily implants in humans. The data that does exist on this matter relates to the animal kingdom, with [56] presenting evidence of direct correlation between implanted RFID chips and cancer. Such headline stories have produced fears that all implants have hidden health risks associated with them. Indeed, in 2004 the acclaimed VeriChip device received unwelcomed attention when the FDA listed multiple health risks associated with their device [57]. Even wearables have hit the headlines with regards to skin rashes generated because of reactions [58]. To add fuel to the fears, [59] have classified wireless devices emitting non ionizing radio frequencies as potential carcinogens; hardly something that people will desire to have implanted into their bodies.

One could extrapolate the available information and conclude that long-term use of implants will lead to tissue reactions at best, and plausibly cancer and other life-threatening illness. Coupling this with the additional practical concerns over hygiene issues during implantation, complications when having MRI scans, x-rays and traveling, and the conceivable likelihood of consumer implanted devices interfering with medically prescribed implants [60], it is easy to see how implantable electronics and sensor networks could rapidly become somewhat of a technological pariah.

Finally, major external factors that could derail success are liberty and religious objections. Most people object strongly to any technology which allows them to effectively be monitored and tracked anywhere in real-time. A number of world religions strictly forbid the practice of tattooing and of cutting the skin, and many fundamental Christians would consider

subcutaneous identification and e-payment sensors as the impious mark of the beast warned about in biblical writings.

None of these issues can be overcome easily as many of the objections are difficult to remedy, thus the technology could struggle to enjoy widespread acceptance.

IV. Summary and Conclusions

Body-implantable devices for non-medical purposes are emerging as a hot topic that has the potential to permeate throughout society. This technology has exceptional hurdles to jump that many other emerging technologies do not. The preceding SWOT analysis has highlighted how this technology could be a great benefit, but also a considerable threat, to future society. If well managed, we could realize a new paradigm in how we work, rest, communicate, play, exercise, age, travel, and shop, with genuine advances in security, entertainment, health, social networking, daily activities, efficiency, commerce, and human body enhancement. This technology will be complemented and enriched by other emerging technologies such as Cloud computing, IoT, and NFC. However, if poorly managed or even mismanaged we could face dystopian societies that better reflect a George Orwell novel, with key issues including risks of implanted devices to user health, personal safety, privacy, identity protection, and co-existence with medically prescribed implants. The technology will typically be opposed due to fears surrounding dehumanisation, human rights, social privacy, and religious objections.

To ensure widespread success of the technology it is imperative that a number of recommendations are universally implemented. Recommendations to protect the potential and to drive the success of this exciting technological era are multifaceted. Such recommendations include the early development of technical regulations which incorporate input and commitment of industry, governments, academics, clinician, and end users, and to develop the technology and standards synergistically with other supporting technologies (IoT, NFC, etc.) to ensure multi-level interoperability. Also, the timely establishment of industrial alliances to safeguard interoperability is of paramount importance, as is engaging the fringe groups to raise the profile, increase acceptability and ensure their valued and unique insight is integrated in a constructive manner. Development of standard clinical procedures for insertion and retrieval of subcutaneous devices is an obvious essential. With regards to the devices, the authors recommend the completion of suitably funded clinical studies to confirm long-term implant safety regarding tissue health, hygiene, electromagnetic scanning (MRI, x-ray), and also the embracement of new bio-materials in which the electronics can be enveloped. Likewise rigorous testing to certify suitable security of devices, networks, data, etc., is essential, as is a failsafe way to update firmware devices in-situ to address arising issues (design flaws, compatibility, circumventing limitations). From a social point of view, recommendations include the carefully managed introduction of the technology in regards to commercial timing, publicity, advertising and use of outcomes from focus groups. Leadership of governments (and subsequent legislation) is similarly essential to guarantee that widespread adoption of technology will not be used (either overtly or covertly) for data collection, monitoring, or control of citizens.

To embed such regulations, standards and practices requires time, effort, deliberate orchestration, and cooperation. When there is a desire to realize a new technological advance developers may take shortcuts and deliver the technology before the appropriate checks and balances are in place. [61] remarked that digital media is often invented, designed, adopted and even celebrated before society is able to understand their impact on lives, culture, art, privacy, and social practices. [60] echoed the same concern for video surveillance technologies, commenting that "*their use and capabilities are increasing, while policies, procedures, and uses for the information that is visually captured for analysis are still evolving*". To deliver all the strengths that subcutaneous consumer electronics have to offer and to save us from all of its threats, society looks to prominent and influential organisations such as the IEEE to develop standards, white papers, and structures to ensure safety and compatibility of devices and systems at every level. We have many challenges ahead to accomplish the reality of implantable systems, but it promises to be a profoundly exciting journey.

References

[1] A. J. Greenspon, et al., "Trends in Permanent Pacemaker Implantation in the United States From 1993 to 2009: Increasing Complexity of Patients and Procedures", Journal of the American College of Cardiology, vol. 60, no. 16, pp. 1540-1545, October 2012.

[2] S. Rao, and J. Chiao, "Body Electric: Wireless Power Transfer for Implant Applications," Microwave Magazine, IEEE, vol. 16, no. 2, pp. 54-64, March 2015.

[3] X. Hei, X. Du, S. Lin, and I. Lee, "PIPAC: Patient infusion pattern based access control scheme for wireless insulin pump system," INFOCOM, 2013 Proceedings IEEE, vol., no., pp. 3030-3038, 14-19 April 2013.

[4] X. Qian, H. Hao, B. Ma, X. Wen, C. Hu and L. Li, "Implanted rechargeable electroencephalography (EEG) device," Electronics Letters, vol. 50, no. 20, pp. 1419-1421, 25 September 2014.

[5] T. Denison, M. Morris, and F. Sun, "Building a bionic nervous system," Spectrum, IEEE , vol. 52, no. 2, pp. 32-39, February 2015.

[6] D. Prattichizzo, F. Chinello, C. Pacchierotti, and M. Malvezzi, "Towards Wearability in Fingertip Haptics: A 3-DoF Wearable Device for Cutaneous Force Feedback," Haptics, IEEE Transactions on , vol. 6, no. 4, pp. 506-516, Oct.-Dec. 2013.

[7] S. Hiremath, G. Yang, and K. Mankodiya, "Wearable Internet of Things: Concept, architectural components and promises for person-centered healthcare," Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference on , vol., no., pp. 304-307, 3-5 Nov. 2014.

[8] P.A. Catherwood, and W.G. Scanlon, "Body-centric antenna positioning effects for off-body UWB communications in a contemporary learning environment," Antennas and Propagation (EuCAP), 2014 8th European Conference on , vol., no., pp. 1571-1574, 6-11 April 2014.

[9] M. Billinghurst, "The glass class: Designing wearable interfaces," Mixed and Augmented Reality (ISMAR), 2014 IEEE International Symposium on , vol., no., pp. 1-2, 10-12 Sept. 2014.

[10] P.A. Catherwood, T Zech, and J. McLaughlin, "Cost-effective RSSI Wi-Fi positioning solution for ambulatory patient monitoring devices", Antennas and Propagation Conference (LAPC), 2010 Loughborough, Loughborough, pp. 557-560, 8-9 Nov. 2010.

[11] A. Miah, "Engineering greater resilience or radical transhuman enhancement?," Bionic Health: Next Generation Implants, Prosthetics and Devices, 2009 IET , vol., no., pp. 1-2, 1 Oct. 2009.

[12] A.W. Astrin, "IEEE standard supports development of innovative body area networks", IEEE Lifesciences Newsletter, June 2013.

[13] C.E. Palazzi, A. Bujari, G. Marfia, and M. Roccetti, "An overview of opportunistic ad hoc communication in urban scenarios," Ad Hoc Networking Workshop (MED-HOC-NET), 2014 13th Annual Mediterranean , vol., no., pp. 146-149, 2-4 June 2014.

[14] A. Bone, N. Fortune, T. Nichols, and N.D. Noah "Body Piercing in England: a Survey of Piercing at Sites Other than Earlobe". British Medical Journal, vol. 336, pp. 1426–1428, 2008.

[15] W. Heywood, et al., "Who Gets Tattoos? Demographic and behavioral Correlates of Ever Being Tattooed in a Representative Sample of Men and Women", Annals of Epidemiology, vol. 22, no. 1, pp. 51–56, January 2012.

[16] S. Braverman, "One in Five U.S. Adults Now Has a Tattoo", The Harris Poll #22, February 23, 2012.

[17] S. Wohlrab, J. Stahl, and P.M. Kappeler, "Modifying the body: Motivations for getting tattooed and pierced", Body Image, vol. 4, pp. 87–95, 2007.

[18] A. Smith. "Biohackers and body modification." Internet:http://www.abc.net.au/radionational/programs/bodysphere/biohackers-and-body-modification/6295194, March 10 2015 [May 22 2015].

[19] D. Schwartzmana, et al., "An off-the-shelf plasma-based material to prevent pacemaker pocket infection", Biomaterials, vol. 60, pp: 1-8, Aug. 2015.

[20] T. Nagaoka, "Large-scale specific absorption rate computation in various people on GPUs," Electromagnetics in Advanced Applications (ICEAA), 2014 Intl. Conf. on , vol., no., pp. 699-702, 3-8 Aug. 2014.

[21] K.R. Foster, and J. Jaeger, "RFID Inside," Spectrum, IEEE, vol. 44, no. 3, pp. 24-29, March 2007.

[22] J.J.S. Norton, et al, "Soft, curved electrode systems capable of integration on the auricle as a persistent brain–computer interface", Proceedings of the National Academy of Sciences, vol. 112, no. 12, March 2015.

[23] C.Q. Choi. "A Brain-Computer Interface That Lasts for Weeks", IEEE Spectrum, March 16 2015.

[24] M. Weigel, T. Lu, G. Bailly, A. Oulasvirta, C. Majidi, and J. Steimle, "iSkin: Flexible, Stretchable and Visually Customizable On-Body Touch Sensors for Mobile Computing", Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '15), 11-18 April 2015.

[25] Jr. William P. Alberth, "Coupling an electronic skin tattoo to a mobile communication device", US Patent WO 2013166377 A1, 7 Nov. 2013. [patent]

[26] L. Xie, and M. Cai, "Human Motion: Sustainable Power for Wearable Electronics," Pervasive Computing, IEEE , vol. 13, no. 4, pp. 42-49, Oct.-Dec. 2014.

[27] F. Macrae. "Superhero vision." Internet: http://www.dailymail.co.uk/sciencetech/article-2952588/Now-SUPERHERO-vision-Contact-lenses-magnify-words-THREE-FOLD-controlled-winking.html, Feb. 14 2015 [May 19 2015].

[28] E. Strickland, "We Will End Disability by Becoming Cyborgs", Spectrum, IEEE, 27 May 2014.

[29] World Health Organization, "A global brief on hypertension. Silent killer, global public health crisis" Geneva, Switzerland: World Health Organization, 2013.

[30] A. Bodhani, "Smartphones pay the price," Engineering & Technology, vol. 6, no. 10, pp. 56-59, November 2011.

[31] C. Manders, "Moving surveillance techniques to sousveillance: Towards equiveillance using wearable computing," Technology and Society (ISTAS), 2013 IEEE International Symposium on , vol., no., pp. 19-19, 27-29 June 2013.

[32] Internet: https://epicenterstockholm.com, [April 28 2015].

[33] B. Kress, and T. Starner, "A review of head-mounted displays (HMD) technologies and applications for consumer electronics", SPIE Proceedings 8720 - Photonic Applications for Aerospace, Commercial, and Harsh Environments, pp: 87200A-87200A-13, May 31, 2013.

[34] C. Harrison, D. Tan, and D. Morris, "Skinput: appropriating the skin as an interactive canvas", Communications of the ACM Magazine, vol. 54, no. 8, pp. 111-118, 2011.

[35] G. McDonald. "Internet Telepathy? Thoughts Transmitted Online.", Internet: http://news.discovery.com/tech/biotechnology/internet-telepathy-thoughts-transmitted-online-140903.htm, Sept 3 2014 [May 19 2015].

[36] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues, "The Security Implications of VeriChip Cloning", Journal of the American Medical Informatics Association, vol. 13, no. 6, pp. 601-607, 2006.

[37] "PIP Breast Implants - Removal and Replacement, NHS Choices." Internet:http://www.nhs.uk/Conditions/Breast-implants/Pages/Removal%20and%20replacement%20of%20PIP%20implants.aspx, July 9 2014 [May 18 2015].

[38] L. Yang, et al., "Unlocking Smart Phone through Handwaving Biometrics," Mobile Computing, IEEE Transactions on , vol. 14, no. 5, pp. 1044-1055, May 1 2015.

[39] M.A. Ali, and S. Mann, "The inevitability of the transition from a surveillance-society to a veillance-society: Moral and economic grounding for sousveillance," Technology and Society (ISTAS), 2013 IEEE Intl. Symposium on, vol., no., pp. 243-254, 27-29 June 2013.

[40] "Materials in Medicine - Institute of Materials, Minerals and Mining." Internet: www.iom3.org/fileproxy/348340, [April 14 2015].

[41] "Implants and Prosthetics." Internet: http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ImplantsandProsthetics, June 6 2014 [May 12 2015].

[42] D. Shunk, "Ethics and the Enhanced Soldier of the near Future", Military Review, vol. 95, no. 1, Feb. 2015.

[43] D. Akinwande, N. Petrone, and J. Hone, "Two-dimensional flexible nanoelectronics", Nature Communication, vol. 5, no. 5678, 2014.

[44] D. Son, et al, "Multifunctional wearable devices for diagnosis and therapy of movement disorders", Nature Nanotechnology, vol. 9, no. 5, pp. 397-404, 2014.

[45] V. Sanchez-Romaguera, et al., "Towards inkjet-printed low cost passive UHF RFID skin mounted tattoo paper tags based on silver nanoparticle inks," Royal Society Chemistry, Journal of Materials Chemestry C, vol. 1, pp. 6395–6402, 2013.

[46] C. Perakslis, K. Michael, M.G. Michael, and R. Gable, "Perceived barriers for implanting microchips in humans: A transnational study," Norbert Wiener in the 21st Century (21CW), 2014 IEEE Conference on , vol., no., pp. 1-8, 24-26 June 2014.

[47] K. Michael, and M.G. Michael. "The Diffusion of RFID Implants for Access Control and ePayments: Case Study on Baja Beach Club in Barcelona", IEEE International Symposium on Technology and Society (ISTAS10), pp. 242-252, 2010.

[48] M.G. Michael, and K. Michael, "Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies". Hershey: PA: IGI Global, 2013.

[49] L. Whitney. "Lenovo hit by lawsuit over Superfish adware." Internet: http://www.cnet.com/uk/news/lenovo-hit-by-lawsuit-over-superfish-adware, Feb. 24 2015 [May 14 2015].

[50] S.A. Applin, and M.D. Fischer, "Watching Me, Watching You. (Process surveillance and agency in the workplace)," Technology and Society (ISTAS), 2013 IEEE International Symposium on , vol., no., pp. 268-275, 27-29 June 2013.

[51] T. Ye, B. Moynagh, R. Albatal, and C. Gurrin, "Negative FaceBlurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass", Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management, vol. no. pp. 2036-2038, 2014.

[52] K. Michael, and M.G. Michael. "No Limits to Watching?" Communications of the ACM 56.11, 2013.

[53] M. Zennie. "Tech pioneer with augmented-reality glasses bolted to his head traps Paris McDonald's workers 'who tried to rip the device off his face'.", Internet: http://www.dailymail.co.uk/news/article-2175062/EyeTap-augmented-reality-pioneer-Steve-Mann-assaulted-Paris-McDonalds-employees.html, July 18 2012 [May 4 2015].

[54] V. Woollaston. "Now THAT'S 'wearable technology'! Man implants a mini computer under his SKIN to track his body temperature." http://www.dailymail.co.uk/sciencetech/article-2487100/Now-THATS-wearable-technology-Man-implants-mini-SKIN-track-body-temperature.html Nov. 4 2013 [May 4 2015].

[55] l. Clark. "Magnet-implanting DIY biohackers pave the way for mainstream adoption", http://www.wired.co.uk/news/archive/2012-09/04/diy-biohacking, Sept. 4 2012 [May 4 2015].

[56] K. Albrecht, "Microchip-induced tumors in laboratory rodents and dogs: A review of the literature 1990–2006," Technology and Society (ISTAS), 2010 IEEE International Symposium on, vol., no., pp. 337-349, 7-9 June 2010.

[57] D. Tillman. "Exhibit 99.2, Evaluation of Automatic Class III Designation VeriChip(TM) Health Information Microtransponder System", Internet: http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt, Oct. 12 2004 [May 15 2015].

[58] “Fitbit says new wearable device can cause skin rash.”, Internet:http://www.bbc.co.uk/news/technology-31438706, Feb. 12 2015 [May 21 2015].

[59] World Health Organisation, Press release no.208, “IARC classifies radiofrequency electromagnetic fields as possibly carcinogenic to humans”, International agency for research on cancer, 31st May, 2011.

[60] B. McPhail, A. Clement, J. Ferenbok, and A. Johnson, “I'll be watching you: Awareness, consent, compliance and accountability in video surveillance,” Technology and Society (ISTAS), 2013 IEEE International Symposium on , vol., no., pp. 276-284, 27-29 June 2013.

[61] I. Pedersen, “Ready to wear (or not): Examining the rhetorical impact of proposed wearable devices,” Technology and Society (ISTAS), 2013 IEEE Intl. Symposium on , vol., no., pp. 201-202, 27-29 June 2013.