INFORMATION SECURITY CONCERNS AS A CATALYST FOR THE DEVELOPMENT OF IMPLANTABLE COGNITIVE NEUROPROSTHESES

Gladden, Matthew E.

Institute of Computer Science, Polish Academy of Sciences (IPI PAN), Warsaw, Poland

ABSTRACT

Standards like the *ISO 27000* series, *IEC/TR 80001*, *NIST SP 1800*, and FDA guidance on medical device cybersecurity define the responsibilities that manufacturers and operators bear for ensuring the information security of implantable medical devices. In the case of implantable cognitive neuroprostheses (ICNs) that are integrated with the neural circuitry of their human hosts, there is a widespread presumption that InfoSec concerns serve only as limiting factors that can complicate, impede, or preclude the development and deployment of such devices. However, we argue that when appropriately conceptualized, InfoSec concerns may also serve as drivers that can spur the creation and adoption of such technologies. A framework is formulated that describes seven types of actors whose participation is required in order for ICNs to be adopted; namely, their 1) producers, 2) regulators, 3) funders, 4) installers, 5) human hosts, 6) operators, and 7) maintainers. By mapping onto this framework InfoSec issues raised in industry standards and other literature, it is shown that for each actor in the process, concerns about information security can either disincentivize or incentivize the actor to advance the development and deployment of ICNs for purposes of therapy or human enhancement. For example, it is shown that ICNs can strengthen the integrity, availability, and utility of information stored in the memories of persons suffering from certain neurological conditions and may enhance information security for society as a whole by providing new tools for military, law enforcement, medical, or corporate personnel who provide critical InfoSec services.

Keywords: *cognitive neuroprosthetics, implantable medical devices, information security, human enhancement, digital health ecosystems, health information systems, ISO 27000 series, ISO 27799, NIST SP 1800*

INTRODUCTION

Developments in the field of neuroprosthetics are occurring at a rapid pace. Among the most revolutionary technologies are implantable cognitive neuroprostheses (ICNs) that are housed permanently within a human host's body and which interact with the brain to regulate or enhance cognitive processes relating to memory, emotion, imagination, belief, and conscious awareness.

If such devices fail to function as intended, they can have a severe negative impact on the psychological and physical well-being of their human hosts. While information security (InfoSec) experts have begun formulating approaches to safeguarding these devices against computer viruses, cyberattacks, communication glitches, power outages, user authentication errors, and other problems that could disrupt their functioning, it is commonly presumed that InfoSec concerns represent a significant obstacle to the broader adoption of such technologies. Almost no consideration has been given to the possibility that InfoSec concerns might also create compelling reasons *in favor of* developing and deploying ICNs within society.

In this text, a conceptual framework is formulated which demonstrates that at each step in the process of creating and adopting ICNs, it is possible for InfoSec-related concerns to either impede the process or drive it forward. Before considering that framework, we can review the state of ICNs and industry standards for information security, especially as it applies to implantable medical devices.

BACKGROUND AND FOUNDATIONS

Overview of Implantable Cognitive Neuroprosthetics

A neuroprosthesis can be understood as "a technological device that is integrated into the neural circuitry of a human being" (Gladden 2015, p. 21; Lebedev, 2014). Such neuroprostheses can be sensory, motor, or cognitive in nature (Lebedev, 2014). In this text we focus on cognitive neuroprostheses – experimental devices that enhance, regulate, replace, or otherwise participate in cognitive processes and phenomena (Gladden, 2015, pp. 26-27) such as memory (Han et al., 2009; Ramirez, 2013), emotion (Soussou and Berger, 2008), personal identity and agency (Van den Berg, 2012), and consciousness (Kourany, 2013; Claussen and Hofmann, 2012).

Such devices are still in their early experimental stages; however, it is anticipated that they will eventually be used to treat a range of conditions such as anxiety disorders, emotional disorders, addictions, Alzheimer's disease, and other memory disorders (Ansari et al., 2007; Merkel et al., 2007; Stieglitz, 2007; Soussou and Berger, 2008; Van den Berg, 2012; Gladden, 2015, pp. 22-26) as well as to enhance cognitive capacities like memory and alertness beyond their natural limits (Spohrer, 2002; McGee, 2008; Brunner and Schalk, 2009; Koops and Leenes, 2012; Kourany, 2013; Rao et al., 2014; Warwick, 2014; Gladden, 2015, pp. 26-28).

Some neuroprosthetic technologies comprise large and sessile pieces of non-invasive equipment (e.g., fMRI machines) that are permanently housed in dedicated medical facilities and can only be used at those locations. Other neuroprosthetic technologies involve prostheses that are physically integrated into the biological organism of a human host but have an interface with the external environment; still others are implants which, after their surgical insertion, are entirely concealed within the body of a human host (often within the brain) and may remain there throughout the rest of their host's lifetime (Gladden, 2015, pp. 28-29). In this text we focus on implantable cognitive neuroprosthetic (ICNs), which display unique InfoSec characteristics because they: 1) are often deeply integrated with the biological neural network of their human host's brain, creating the possibility of severe psychological or physical harm (including death) if they are compromised or fail to function as intended; 2) must rely on wireless communication to interact with external health information systems and receive instructions and software updates; and 3) are highly mobile devices that enter a diverse range of unpredictable and unsecure environments as their host goes about his or her daily life (*ISO 27799*, 2008, p. 47; *NIST SP 1800-1a*, 2016, p. 1; *Content of Premarket Submissions*, 2014, p. 4; Gladden, 2015, pp. 62-65).

Fundamental Principles of Information Security (InfoSec)

Information security is an interdisciplinary field whose goal has traditionally been to ensure the *confidentiality*, *integrity*, and *availability* of information (Rao and Nayak, 2014, pp. 49-53; *NIST SP 1800-1b*, 2016, p. 9; "Security Risk Assessment Framework," 2014). This notion of a 'CIA Triad' has been expanded through Parker's vision of safeguarding the three additional attributes of the *possession*, *authenticity*, and *utility* of information (Parker, 2002; Parker, 2010). However, a neuroprosthetic device is not a conventional computerized information system; as an instrument integrated into the neural circuitry of its human host, it becomes part of the personal 'information system' that comprises the host's mind and body and which possesses a unique legal and moral status. As a result, ensuring information security for a neuroprosthesis also entails safeguarding the three additional attributes of *distinguishability,* or the possibility of differentiating information according to its nature or origin (e.g., the ability to recognize which of the thoughts experienced in one's mind are 'one's own' and which, if any, are being generated or altered by a neural implant); *rejectability,* or the ability of a host-device system to purposefully exclude particular information from the host's conscious awareness (i.e., the freedom *not* to recall certain memories or entertain particular thoughts at a given moment); and *autonomy*, or the ability of a host-device system to exercise its own agency in the processing of information (i.e., the ability to arrive at a decision through the use of one's own cognitive processes and of one's own volition, without the contents of that decision being manipulated or determined by some external agent) (Gladden, 2015, pp. 138-42). In the case of a neuroprosthetic device integrated with the neural circuitry of its human host, information security thus involves not only securing all electronic data stored in or processed by the device but also ensuring the integrity of the thoughts, memories, volitions, emotions, and other informational processes and content of the natural biological portions of the host's mind in the face of a full range of vulnerabilities and threats including electronically, biologically, and psychologically based attacks (Gladden, 2015, pp. 40-57; Denning et al., 2009).

A key mechanism for promoting information security is the implementation of administrative, physical, and logical security controls (Rao and Nayak, 2014, pp. 66-69). This does not simply involve the installation of antivirus software but rather the creation and effective implementation of a comprehensive program of risk management (*NIST SP 800-33*, 2001, p. 19).

InfoSec Standards of Relevance to Implantable Cognitive Neuroprosthetics

Widely utilized standards that help organizations design and implement best practices for information security include the *ISO 27000* series that defines requirements for InfoSec management systems or ISMSes (*ISO/IEC 27001*, 2013) and a code of practice for InfoSec controls (*ISO/IEC 27002*, 2013). Similarly, NIST standards address risk management and InfoSec life cycles (*NIST SP 800-37*, 2010), InfoSec practices for managers (*NIST SP 800-100*, 2006), and security and privacy controls (*NIST SP 800-53, 2013*).

Beyond these generic InfoSec standards, national and international bodies are increasingly developing specialized standards relating to health care data and medical devices. For example, ISO has published standards and other resources relating to InfoSec for remotely maintained medical devices and information systems (*ISO/TR 11633*, 2009), IT networks that incorporate medical devices (the *IEC 80001* series, 2010-15), and InfoSec management in the field of health care (*ISO 27799*, 2008). In 2015, the NIST issued a draft publication on information security for health records stored or processed on mobile devices (*NIST SP 1800-1*). The US Food and Drug Administration has issued guidance relating to cybersecurity for medical devices utilizing off-the-shelf software (2005) and to the premarket (2014) and postmarket (2016) management of cybersecurity for medical devices. Industry organizations such as the Medical Device Privacy Consortium have proposed their own InfoSec standards (*Security Risk Assessment Framework for Medical Devices*, 2014).

These resources do not focus specifically on the InfoSec questions that arise with the use of ICNs. However, those questions have been explored from an academic perspective in works such as those by McGee (2008), Denning et al. (2009), Koops and Leenes (2012), Kosta and Bowman (2012), and Gladden (2015). By interpreting the published standards in light of such scholarship, it is possible to identify specific InfoSec concerns of relevance to the stakeholders whose participation is required for the implementation of ICNs.

FORMULATING A CONCEPTUAL FRAMEWORK FOR INFOSEC CONCERNS AS AN IMPEDIMENT OR IMPETUS TO THE DEVELOPMENT OF ICNS

In order to identify ways in which InfoSec concerns can either drive or impede the adoption of ICNs, we propose a conceptual framework that incorporates two dimensions: 1) the chain of actors who participate in the development and adoption of such technologies; and 2) their disincentivization or incentivization to participate in that process as a result of InfoSec considerations. Note that many other factors may influence whether actors decide to pursue the development of ICNs, including ethical, legal, public policy, financial, and operational considerations; the framework formulated here only attempts to identify those factors relating to information security. We can consider the framework's dimensions in more detail.

First Dimension: Actors in the Process of Neuroprosthetic Devices' Adoption

Review of the InfoSec literature for medical devices makes it possible to identify seven types of stakeholders whose participation will be required in order for any implantable neuroprosthetic technology to be developed and deployed in human hosts and whose failure to implement effective InfoSec measures could potentially result in injury or death for an ICN's host (*Content of Premarket Submissions*, 2014, p. 3; Gladden, 2015, pp. 109-110; *Postmarket Management of Cybersecurity*, 2016, p. 10). These actors include: 1) the designers and manufacturers of neuroprosthetic hardware and software (i.e., its 'producers'); 2) the government agencies and licensing bodies that must authorize the use of cognitive neuroprostheses in order for it to be legal (the technology's 'regulators'); 3) the government health services and private insurers that bear the cost of such devices' surgical implantation and ongoing maintenance ('funders'); 4) hospitals, clinics, and physicians who assess individual patients and perform the implantation of neuroprosthetic devices ('installers'); 5) the human subjects in whom neuroprosthetic devices are implanted but who may or may not actually operate the devices ('hosts'); 6) the typically institutional service providers that manage devices' connections to external systems and may remotely manage the devices themselves (their 'operators'); and 7) the providers of physical maintenance and upgrades, software updates, and additional functionality for neuroprosthetic devices already in use (their 'maintainers').

Collectively, the first two types of stakeholders (producers and regulators) can be understood as enabling the *creation* of implantable cognitive neuroprosthetic devices; the following three types (funders, installers, and hosts) as enabling their *implantation;* and the final two types (operators and maintainers) as enabling their *ongoing use*.

Second Dimension: Disincentivization or Incentivization of Participation in Adoption Process

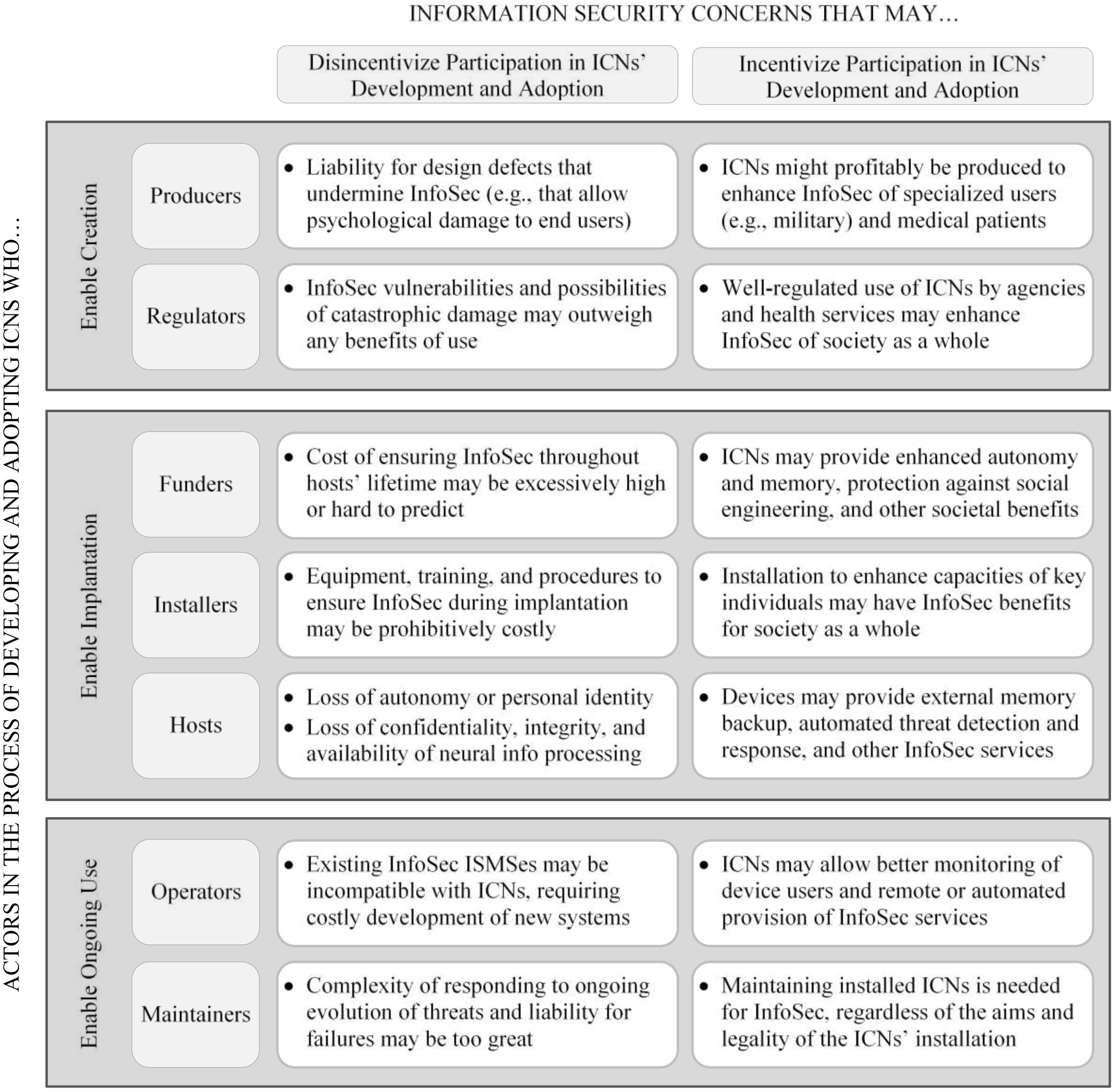
For a given actor, InfoSec concerns may provide the actor with either disincentives or incentives (or both) to participate in the development and adoption of ICNs.

DISCUSSION OF POTENTIAL INFOSEC-RELATED DISINCENTIVES AND INCENTIVES FOR EACH OF THE ACTOR TYPES TO PARTICIPATE IN ICN DEVELOPMENT

By combining both dimensions, a two-dimensional framework is created; Figure 1 presents such a framework that has been populated with sample InfoSec concerns drawn from industry standards and other literature. We can now explore conceptually how for each of the potential actors in the process, InfoSec concerns can create either a disincentive or incentive for the actor to participate in the development and adoption of ICNs.

Producers: Designers and Manufacturers of Hardware and Software

Designers and manufacturers are largely responsible for the InfoSec characteristics of ICNs (*Content of Premarket Submissions*, 2014, p. 1). The reliance of implantable neuroprostheses on mobile, wireless, and networked technologies places them at significant danger for the embedding of malicious code and other attacks that can exploit vulnerabilities in such technologies (*ISO 27799*, 2008, p. 47; *NIST SP 1800-1a*, 2016, p. 1; *Content of Premarket Submissions*, 2014, p. 4). InfoSec breaches could have fatal consequences for the human hosts of ICNs (*ISO 27799*, 2008, p. 47); large-scale catastrophic InfoSec failures attributable to a manufacturer could result in massive fines and remediation costs, irreparable reputation brand damage, and even bankruptcy ("Security Risk Assessment Framework," 2014, p. 16). Producers may thus decide that the risks inherent in producing ICNs outweigh any possible benefits.



INFORMATION SECURITY CONCERNS THAT MAY…

ACTORS IN THE PROCESS OF DEVELOPING AND ADOPTING ICNS WHO…

		Disincentivize Participation in ICNs' Development and Adoption	Incentivize Participation in ICNs' Development and Adoption
Enable Creation	Producers	• Liability for design defects that undermine InfoSec (e.g., that allow psychological damage to end users)	• ICNs might profitably be produced to enhance InfoSec of specialized users (e.g., military) and medical patients
	Regulators	• InfoSec vulnerabilities and possibilities of catastrophic damage may outweigh any benefits of use	• Well-regulated use of ICNs by agencies and health services may enhance InfoSec of society as a whole
Enable Implantation	Funders	• Cost of ensuring InfoSec throughout hosts' lifetime may be excessively high or hard to predict	• ICNs may provide enhanced autonomy and memory, protection against social engineering, and other societal benefits
	Installers	• Equipment, training, and procedures to ensure InfoSec during implantation may be prohibitively costly	• Installation to enhance capacities of key individuals may have InfoSec benefits for society as a whole
	Hosts	• Loss of autonomy or personal identity • Loss of confidentiality, integrity, and availability of neural info processing	• Devices may provide external memory backup, automated threat detection and response, and other InfoSec services
Enable Ongoing Use	Operators	• Existing InfoSec ISMSes may be incompatible with ICNs, requiring costly development of new systems	• ICNs may allow better monitoring of device users and remote or automated provision of InfoSec services
	Maintainers	• Complexity of responding to ongoing evolution of threats and liability for failures may be too great	• Maintaining installed ICNs is needed for InfoSec, regardless of the aims and legality of the ICNs' installation

Figure 1. *Figure 1. Examples of InfoSec-related concerns synthesized from InfoSec standards and literature that could potentially disincentivize or incentivize participation of seven key types of actors whose involvement is necessary in order for implantable cognitive neuroprostheses (ICNs) to be developed and deployed.*

Moreover, the unique nature of ICNs may create contradictory InfoSec-related design requirements which are infeasible for manufacturers to satisfy simultaneously. For example, devices allowing access to neural functions must be maximally secure while at the same time granting full and immediate access to medical personnel in case of an emergency (*Content of Premarket Submissions*, 2014, p. 4). Similarly, for ICNs that store data in a biological or biomimetic neural network (see Merkel et al., 2007; Rutten et al., 2007; Stieglitz, 2007; Gladden, 2015, p. 31) or which transmit data through synaptic connections with biological neurons, it may be impossible to utilize the InfoSec best practice of encrypting data (*NIST SP 1800-1e*, 2016, p. 5) without destroying the information's availability and utility.

Despite these concerns, though, it is possible that some individuals or organizations may wish to employ ICNs precisely in order to enhance their own information security or to protect that of others. In such a case, InfoSec considerations would constitute a factor driving demand for ICNs, which could make their development and production profitable and desirable for device designers and manufacturers. Such potential uses for individuals include strengthening the agency of users whose autonomy has been reduced by disorders such as Parkinson's disease (Van den Berg, 2012; Gladden, 2015, pp. 97, 150-51), restoring the memory mechanisms of individuals suffering from Alzheimer's disease or other neurological disorders (Ansari et al., 2007; Han et al., 2009; Ramirez et al., 2013; McGee, 2008; Warwick, 2014, p. 267), and providing the ability to record and 'play back' audiovisual experiences at will with perfect fidelity (Merkel et al., 2007; Robinett, 2002; McGee, 2008, p. 217; Gladden, 2015, pp. 156-57). Potential uses for organizations include augmenting the brains of military personnel to aid in their work of gathering and processing intelligence and engaging in cyberwarfare and combat operations (Schermer, 2009; Brunner & Schalk, 2009; Gladden, 2015, p. 34) and to enhance the availability of sensory information and memories by reducing their need for sleep (Kourany, 2013; Gladden, 2015, p. 151).

Regulators: Agencies and Licensing Bodies Authorizing Device Adoption

Regulatory agencies may be hesitant to approve the use of ICNs – especially for purposes of elective enhancement – if their InfoSec characteristics create a grave and widespread danger of psychological, physical, economic, or social harm for their users without counterbalancing benefits. However, regulators may be willing to authorize at least limited development of ICNs if they potentially create new and more effective tools for use by police personnel to analyze crime-related data and combat cybercrime, by military personnel to gather intelligence and conduct cyberwarfare, or by the personnel of private enterprises to detect and combat corporate espionage and cyberattacks (Gladden, 2015, p. 111). Regulation may also be desirable in order to create and enforce national or international InfoSec standards that, for example, allow emergency access to ICNs by medical personnel (Cho & Lee, 2012; Freudenthal et al., 2007; Gladden, 2015, p. 273).

Funders: Government Health Services and Insurers Subsidizing Device Use

The ongoing and unpredictable costs of protecting ICNs' human hosts from cyberattacks throughout the rest of their lives and of caring for those rendered psychologically, physically, or economically damaged as a result of such attacks may contribute to decisions by public health services and insurers that subsidizing the implantation and use of ICNs – especially those employed for elective enhancement – is not a sound investment.

On the other hand, institutions such as national governments and large corporations may be willing to fund the use of ICNs by their own personnel if the devices would be utilized to enhance the information security of those institutions or the constituencies they serve – such as when used by specialized military, police, health care, or corporate business intelligence and InfoSec personnel ("Bridging the Bio-Electronic Divide," 2016; Szoldra, 2016). Moreover, expenditures enabling the successful widespread use of ICNs to treat disorders such as Alzheimer's disease (Ansari et al., 2007) could be understood as enhancing the 'information security' of significant populations within society (e.g., by increasing the integrity, availability, and utility of memories and other information available to affected individuals and the autonomy of such human beings as host-device systems) and could potentially be justified by government health services on the grounds of improving public health and generating long-term savings on health care costs.

Installers: Hospitals and Physicians Who Implant Devices

Small clinics or hospitals with great expertise in performing surgical procedures may not possess equivalent expertise in information security (*ISO 27799*, 2008, p. v), making it impossible for them to ensure adequate information security during the preparatory, surgical, and recovery stages of an ICN implantation.

However, the implantation of ICNs by hospitals and physicians to treat disorders such as Alzheimer's and Parkinson's diseases (Ansari et al., 2007; Van den Berg, 2012), treat emotional and psychological disorders (McGee, 2008, p. 217), and regulate levels of conscious alertness (Claussen & Hofmann, 2012; Kourany, 2013, pp. 992-93) could help fulfill their duty of care by enhancing the availability and integrity of patients' information and the autonomy of the patients' host-device systems. Possession of ICNs by a hospital's medical personnel could also enhance the availability of information for those personnel by, e.g., providing instantaneous, hands-free access to online reference texts (Gladden, 2015, pp. 33, 156-57; McGee, 2008) or real-time advice from other medical personnel (Rao et al., 2014; Gladden, 2015, pp. 32-33). It has been estimated that effective InfoSec practices in fields like health care can increase organizational performance by up to 2% (*ISO 27799*, 2008, p. vi); if the use of ICNs by medical personnel would enhance their institutions' InfoSec performance, there may thus be managerial and financial incentives for their deployment, beyond any directly health-related rationales.

Hosts: Human Subjects and End Users of Neuroprosthetic Devices

The human hosts of ICNs subject themselves to the potential introduction of computer viruses, worms, or malware (*ISO 27799*, 2008, p. 45; "Cybersecurity for Medical Devices," 2013, p. 1) into their own cognitive processes and make their own thoughts and memories potential targets for attacks by hackers and other adversaries (*ISO 27799*, 2008, p. 45; Denning et al., 2009; Gladden, 2015). InfoSec failures relating to a host's ICN could result in a loss of autonomy and personal identity; psychological, physical, economic, or social harm; or potentially even the host's death (*ISO 27799*, 2008, p. 5; Gladden, 2015, pp. 145-68).

At the same time, particular human beings may have an incentive to acquire and utilize ICNs in order to combat the effects of Alzheimer's disease, Parkinson's disease, emotional disorders, sleep disorders, and other conditions that negatively impact the integrity and availability of memories stored within their brains and the integrity and autonomy of the ongoing information-processing activities of the individuals' minds (Ansari et al., 2007; Van den Berg, 2012; McGee, 2008, p. 217; Claussen & Hofmann, 2012; Kourany, 2013, pp. 992-93; Soussou and Berger, 2008; Gladden, 2015, pp. 26-27). Individuals may also be able to use ICNs to enhance their information security beyond what is naturally possible for human beings – such as by artificially increasing the quantity and quality of external information accessible to their minds (Koops and Leenes, 2012; Merkel et al., 2007; Robinett, 2002; McGee, 2008, p. 217; Gladden, 2015, pp. 156-57) or enhancing their 'internal' memory capacity beyond natural limits (Spohrer, 2002; McGee, 2008; Warwick, 2014, p. 267; Gladden, 2015, pp. 33, 148).

Operators: Managers of Systems That Monitor and Control Devices

ICNs may create residual risks that the operators of ICN systems are not able to mitigate through the implementation of compensating controls and which may endanger ICNs' 'essential clinical performance' (see *Postmarket Management of Cybersecurity*, 2016, pp. 9, 15). For example, given an ICN's implantable nature, it may be impossible to maintain a secure physical perimeter around the device (*ISO 27799*, 2008, p. 29) and protect it from electromagnetic radiation and other potentially disruptive environmental emissions (*ISO 27799*, 2008, p. 30). For ICNs that store and process data in the form of a biological or biomimetic neural network, it may be impractical or even impossible to regularly back up the devices' data in its entirety to a location that is physically secure in order to ensure its long-term availability (*ISO 27799*, 2008, p. 32; Gladden, 2015, p. 236). Potential operators may also decide not to deploy or support ICNs due to the fact that the organizations' standard InfoSec practices cannot be applied to such devices. For example, operators of a health information system might typically limit network bandwidth for a compromised device or throttle its functionality in order to prevent it from degrading system services otherwise misusing system resources (*ISO 27799*, 2008, p. 46); such a response may be impermissible if it would endanger the human host of a compromised ICN – who may not even be responsible for his or her device's excessive resource demand.

On the other hand, public health services may choose to operate ICN systems precisely in order to enhance the information security of patients suffering from cognitive disorders that disrupt the brain's ability to store or use information (Ansari et al., 2007; Han et al., 2009; Ramirez et al., 2013; McGee, 2008; Warwick, 2014, p. 267; Soussou and Berger, 2008). Operators of ICN systems might also include government military or police agencies, large corporations, or other institutions for which maximizing information security and combatting InfoSec threats is a critical organizational objective; in particular, personnel augmented by such devices could be more effective at gathering and analyzing intelligence and protecting organizations from cyberattacks (Schermer, 2009; Brunner & Schalk, 2009; Gladden, 2015, p. 34). In the case of individual senior political figures or corporate executives, implantation of an ICN may be warranted in order to counteract the effects of Alzheimer's disease, Parkinson's disease, or other cognitive disorders that could impair the individuals' information security and thereby imperil the mission of the institutions in which they work (see Gladden, 2015, pp. 144, 213, 216-17).

Maintainers: Providers of Software Updates and Physical Maintenance Services

Organizations (including third-party businesses) that provide physical maintenance services, antivirus software and updates, and other applications, upgrades, or accessories to expand the functionality of ICNs may be constrained in their ability to access necessary device functions and data due to legal restrictions regarding the privacy of personal health information (*ISO 27799*, 2008, p. 24) that bind the devices' installers and operators. Moreover, maintenance errors by third-party service providers can open a device to attacks (*ISO 27799*, 2008, p. 48) and create liability for those service providers. Such service providers recognize that a 'masquerade' committed by their own personnel to obtain unauthorized information relating to an ICN (either for financial reasons, to advance hacktivism, out of curiosity, or for other purposes) is also a very real danger (*ISO 27799*, 2008, p. 45); in the case of ICNs, the chance that such InfoSec breaches would cause severe psychological or physical harm to a device's host creates risks that service providers may be unwilling to bear.

Regardless of how and why ICNs have been implanted, though, the provision of effective maintenance and upgrade services is necessary in order to protect their users' lives and ensure their information security (*Postmarket Management of Cybersecurity*, 2016) – thus creating a potentially profitable market for such services. In the absence of regular maintenance and upgrades, ICNs would be vulnerable to new and evolving threats – which is an especially critical problem in the case of devices that are so closely integrated with their hosts' brain functions.

CONCLUSION

Many factors determine whether and how quickly particular new biotechnologies are developed and deployed. There is a widespread presumption that the need to ensure information security for organizations and individuals can create obstacles that *impede* or *disallow* the adoption of sensitive biotechnologies but that it cannot *accelerate* or *facilitate* the adoption of such technologies. It is rarely acknowledged by researchers, regulators, or industry practitioners that the desire for information security might itself potentially help drive the development and implementation of technologies such as implantable cognitive neuroprostheses. Thus the Medical Device Privacy Consortium argues, for example, that information security concerns "threaten to disrupt critical information flows to and from medical device companies" ("Welcome," *Deviceprivacy.org*, 2016), and the FDA contends that effective cybersecurity is needed to safeguard the functionality of implantable devices (*Content of Premarket Submissions*, 2014, p. 1). In the policy statements, standards, and outreach campaigns of such leading bodies there is no hint that the converse might also be true – i.e., that properly designed and functioning ICNs and other implantable devices might be deployed precisely for the purpose of safeguarding and enhancing information security of individual users, organizations, or sizeable populations within human society.

By applying the framework developed in this paper to analyze issues raised in industry standards and scholarly literature, we have shown that when 'information security' is appropriately understood in its full sense of assuring the confidentiality, integrity, availability, possession, authenticity, utility, distinguishability, rejectability, and autonomy of information and information systems, for each of the actors involved in the process of developing and deploying ICNs it is possible for InfoSec concerns to serve either as an obstacle that discourages an actor from taking part *or* as a driving factor that encourages an actor to participate in the development and adoption of ICNs. This is true despite – or perhaps because of – the fact that among all forms of implantable devices, ICNs are those that are most intimately integrated with the neural circuitry of their human hosts and which are able to most directly participate in cognitive processes that are critical for their hosts' psychological and physical well-being. It is our hope that conceptual frameworks such as the one developed here can serve as a basis for further theoretical and empirical studies to explore the ways in which InfoSec concerns can either hinder or impel the adoption of ICNs and other potentially revolutionary biotechnologies.

REFERENCES

Ansari, S., Chaudhri, K., and Al Moutaery, K. (2007), "Vagus Nerve Stimulation: Indications and Limitations," in Sakas, D.E., and Simpson, B.A. (Eds.), *Operative Neuromodulation*, Springer Vienna, pp. 281-86.

"Bridging the Bio-Electronic Divide" (2016), Defense Advanced Research Projects Agency, January 19, 2016, http://www.darpa.mil/news-events/2015-01-19 (accessed May 6, 2016).

Brunner, P., and Schalk, G. (2009), "Brain-Computer Interaction," in Schmorrow, D.D., Estabrooke, I.V., and Grootjen, M. (Eds.), *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, Springer Berlin Heidelberg, pp. 719-23.

Cho, K., and Hoon Lee, D. (2012), "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks," in Jung, S., and Yung, M. (Eds.), *Information Security Applications*, Springer Berlin Heidelberg, pp. 203-18.

Claussen, J.C., and Hofmann, U.G. (2012), "Sleep, Neuroengineering and Dynamics," *Cognitive Neurodynamics,* Vol. 6, No. 3, pp. 211-14.

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (2014), Silver Spring, MD: US Food and Drug Administration.

Denning, T. Matsuoka, Y., and Kohno, T. (2009), "Neurosecurity: Security and Privacy for Neural Devices," *Neurosurgical Focus*, Vol. 27, No. 1: E7.

Freudenthal, E., Spring, R., and Estevez, L. (2007), "Practical techniques for limiting disclosure of RF-equipped medical devices," in *Engineering in Medicine and Biology Workshop, 2007 IEEE Dallas*, IEEE, pp. 82-85.

Gladden, M.E. (2015), *The Handbook of Information Security for Advanced Neuroprosthetics*, Indianapolis: Synthypnion Academic.

Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (2005), Silver Spring, MD: US Food and Drug Administration.

Han, J.-H., Kushner, S.A., Yiu, A.P., Hsiang, H.-W., Buch, T., Waisman, A., Bontempi, B., Neve, R.L., Frankland, P.W., and Josselyn, S.A. (2009), "Selective Erasure of a Fear Memory," *Science* 323, No. 5920, pp. 1492-96.

IEC 80001: Application of risk management for IT-networks incorporating medical devices, Parts 1 through 2-7 (2010-15), ISO/TC 215, Geneva: IEC.

ISO 27799:2008: Health informatics – Information security management in health using ISO/IEC 27002 (2008), ISO/TC 215, Geneva: IEC.

ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements (2013), ISO/IEC JTC 1/SC 27, Geneva: ISO/IEC.

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls (2013), ISO/IEC JTC 1/SC 27, Geneva: ISO/IEC.

ISO/TR 11633-1:2009: Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis (2009), ISO/TC 215, Geneva: ISO.

ISO/TR 11633-2:2009: Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 2: Implementation of an information security management system (ISMS) (2009), ISO/TC 215, Geneva: ISO.

Koops, B.-J., and Leenes, R. (2012), "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes," in Gasson, M.N., Kosta, E., and Bowman, D.M. (Eds.), *Human ICT Implants: Technical, Legal and Ethical Considerations*, T. M. C. Asser Press, pp. 113-34.

Kosta, E., and Bowman, D.M. (2012), "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants," in Gasson, M.N., Kosta, E., and Bowman, D.M. (Eds.), *Human ICT Implants: Technical, Legal and Ethical Considerations*, T. M. C. Asser Press, pp. 97-112.

Kourany, J.A. (2013), "Human enhancement: Making the debate more Productive," *Erkenntnis,* Vol. 79, No. 5, pp. 981-98.

Lebedev, M. (2014), "Brain-Machine Interfaces: An Overview," *Translational Neuroscience* Vol. 5, No. 1, pp. 99-110.

McGee, E.M. (2008), "Bioelectronics and Implanted Devices," in Gordijn, B., and Chadwick, R. (Eds.), *Medical Enhancement and Posthumanity*, Springer Netherlands, pp. 207-24.

Merkel, R., Boer, G., Fegert, J., Galert, T., Hartmann, D., Nuttin, B., and Rosahl, S. (2007), "Central Neural Prostheses," in *Intervening in the Brain: Changing Psyche and Society*, Springer Berlin Heidelberg, pp. 117-60.

NIST Special Publication 1800-1: Securing Electronic Health Records on Mobile Devices (Draft), Parts a, b, c, d, and e (2015), O'Brien, G., Lesser, N., Pleasant, B., Wang, S., Zheng, K., Bowers, C., Kamke, K., and Kauffman, L. (Eds.), Gaithersburg, Maryland: National Institute of Standards & Technology.

NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers (2006), Bowen, P., Hash, J., and Wilson, M. (Eds.), Gaithersburg, Maryland: National Institute of Standards & Technology.

NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security (2001), Stoneburner, G. (Ed.), Gaithersburg, Maryland: National Institute of Standards & Technology.

NIST Special Publication 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (2010), Joint Task Force Transformation Initiative, Gaithersburg, Maryland: National Institute of Standards & Technology.

NIST Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (2013), Joint Task Force Transformation Initiative. Gaithersburg, Maryland: National Institute of Standards & Technology.

Parker, D. (2010), "Our Excessively Simplistic Information Security Model and How to Fix It," *ISSA Journal,* July 2010, pp. 12-21.

Parker, D.B. (2002), "Toward a New Framework for Information Security," in Bosworth, S., and Kabay, M.E. (Eds.), *The Computer Security Handbook*, 4th Ed., John Wiley & Sons.

Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (2016), Silver Spring, MD: US Food and Drug Administration.

Ramirez, S., Liu, X., Lin, P.-A., Suh, J., Pignatelli, M., Redondo, R.L., Ryan, T.J., and Tonegawa, S. (2013), "Creating a False Memory in the Hippocampus." *Science* 341, No. 6144, pp. 387-91.

Rao, R.P.N., Stocco, A., Bryan, M., Sarma, D., Youngquist, T.M., Wu, J., and Prat, C.S. (2014), "A direct brain-to-brain interface in humans," *PLoS ONE* 9, No. 11.

Rao, U.H., and Nayak, U. (2014), *The InfoSec Handbook*, New York: Apress.

Robinett, W. (2002), "The consequences of fully understanding the brain," in Roco, M.C., and Bainbridge, W.S. (Eds.), *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*, Arlington, Virginia: National Science Foundation, pp. 166-70.

Rutten, W.L.C., Ruardij, T.G., Marani, E., and Roelofsen, B.H. (2007), "Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe," in Sakas, D.E., and Simpson, B.A. (Eds.), *Operative Neuromodulation,* Springer Vienna, pp. 547-54.

Schermer, M. (2009), "The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction," *NanoEthics* Vol. 3, No. 3, pp. 217-30.

"Security Risk Assessment Framework for Medical Devices" (2014), Washington, DC: Medical Device Privacy Consortium.

Soussou, W.V., and Berger, T.W. (2008), "Cognitive and Emotional Neuroprostheses," in *Brain-Computer Interfaces*, Springer Netherlands, pp. 109-23.

Spohrer, J. (2002), "NBICS (Nano-Bio-Info-Cogno-Socio) Convergence to Improve Human Performance: Opportunities and Challenges," in Roco, M.C., and Bainbridge, W.S. (Eds.), *Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science*, Arlington, Virginia: National Science Foundation, pp. 101-17.

Stieglitz, T. (2007), "Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems," in Sakas, D.E., and Simpson, B.A. (Eds.), *Operative Neuromodulation,* Springer Vienna, pp. 435-42.

Szoldra, P. (2016), "The government's top scientists have a plan to make military cyborgs," Tech Insider, January 22, 2016, http://www.techinsider.io/darpa-neural-interface-2016-1 (accessed May 6, 2016).

Van den Berg, B. (2012), "Pieces of Me: On Identity and Information and Communications Technology Implants," in Gasson, M.N., Kosta, E., and Bowman, D.M. (Eds.), *Human ICT Implants: Technical, Legal and Ethical Considerations*, T. M. C. Asser Press, pp. 159-73.

Warwick, K. (2014), "The cyborg revolution," *Nanoethics* 8, pp. 263-73.

"Welcome," Medical Device Privacy Consortium, http://deviceprivacy.org (accessed May 6, 2016).