frontiers in Neuroscience

PERSPECTIVE
published: 07 November 2017
doi: 10.3389/fnins.2017.00605

An Axiology of Information Security for Futuristic Neuroprostheses: Upholding Human Values in the Context of Technological Posthumanization

*Matthew E. Gladden**

Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland

Previous works exploring the challenges of ensuring information security for neuroprosthetic devices and their users have typically built on the traditional InfoSec concept of the "CIA Triad" of confidentiality, integrity, and availability. However, we argue that the CIA Triad provides an increasingly inadequate foundation for envisioning information security for neuroprostheses, insofar as it presumes that (1) any computational systems to be secured are merely instruments for expressing their human users' agency, and (2) computing devices are conceptually and practically separable from their users. Drawing on contemporary philosophy of technology and philosophical and critical posthumanist analysis, we contend that futuristic neuroprostheses could conceivably violate these basic InfoSec presumptions, insofar as (1) they may alter or supplant their users' biological agency rather than simply supporting it, and (2) they may structurally and functionally fuse with their users to create qualitatively novel "posthumanized" human-machine systems that cannot be secured as though they were conventional computing devices. Simultaneously, it is noted that many of the goals that have been proposed for future neuroprostheses by InfoSec researchers (e.g., relating to aesthetics, human dignity, authenticity, free will, and cultural sensitivity) fall outside the scope of InfoSec as it has historically been understood and touch on a wide range of ethical, aesthetic, physical, metaphysical, psychological, economic, and social values. We suggest that the field of axiology can provide useful frameworks for more effectively identifying, analyzing, and prioritizing such diverse types of values and goods that can (and should) be pursued through InfoSec practices for futuristic neuroprostheses.

Keywords: information security, CIA triad, neuroprostheses, human-computer interaction, technological posthumanization, philosophy of technology, axiology

OPEN ACCESS

Edited by:
Fivos Panetsos,
Complutense University of Madrid,
Spain

Reviewed by:
Leslie Samuel Smith,
University of Stirling, United Kingdom
Neil R. Smalheiser,
University of Illinois at Chicago,
United States

****Correspondence:***
Matthew E. Gladden
matthew.e.gladden@gmail.com

Specialty section:
This article was submitted to
Neuroprosthetics,
a section of the journal
Frontiers in Neuroscience

Received: *31 August 2017*
Accepted: *16 October 2017*
Published: *07 November 2017*

Citation:
Gladden ME (2017) An Axiology of Information Security for Futuristic Neuroprostheses: Upholding Human Values in the Context of Technological Posthumanization.
Front. Neurosci. 11:605.
doi: 10.3389/fnins.2017.00605

INTRODUCTION

The Unique Information Security Needs of Neuroprostheses

Generic information security (InfoSec) mechanisms like antivirus software and file encryption tools that are useful for safeguarding desktop computers are often inapplicable or unsound for use in securing complex medical technologies. Researchers have thus sought to develop more tailored InfoSec practices for medical information systems (Bergamasco et al., 2001; Freudenthal et al., 2007; Clark and Fu, 2012) and implantable medical devices (Denning et al., 2008, 2010;

Halperin et al., 2008; Rasmussen et al., 2009; Hansen and Hansen, 2010; Schechter, 2010; Hei and Du, 2011; Cho and Lee, 2012; Rotter and Gasson, 2012; Zheng et al., 2014). Similarly, researchers have sought to identify unique InfoSec challenges posed by neuroprosthetic devices, which—due to their integration with the human nervous system—require specialized InfoSec mechanisms that are irrelevant for other types of IMDs (Denning et al., 2009; Bonaci, 2015; Bonaci et al., 2015a,b).

The Difficulty of Formally Defining the Goals of Information Security

Such research only infrequently explores the question of exactly what is meant by "information security." How would one recognize whether efforts to achieve it are succeeding or failing? The majority of texts noted above do not explicitly endorse any existing InfoSec frameworks that formally define goals for information security. Those texts that do explicitly base their analysis on an established definition of information security (Denning et al., 2008, 2009; Halperin et al., 2008; Bonaci, 2015; Bonaci et al., 2015a,b) opt for the classic "CIA Triad," which was developed in the 1970s and establishes *confidentiality*, *integrity*, and *availability* as the three overarching aims of information security. Here "confidentiality" means that disclosure of information is successfully limited to authorized parties, "integrity" means that information is protected from degradation or illicit manipulation, and "availability" means that information can be accessed by authorized users in a timely and reliable manner (Samonas and Coss, 2014).

Selecting the CIA Triad as a conceptual foundation is reasonable, as it is the simplest and best-known InfoSec framework that explicates information security's goals. However, while its value as a pedagogical tool for introducing basic InfoSec principles remains unsurpassed, within the field of InfoSec the CIA Triad's limitations as an instrument for designing comprehensive security practices have gradually become apparent. InfoSec researchers have thus proposed more nuanced frameworks to capture additional aspects of information security (Samonas and Coss, 2014). For example, the Parkerian Hexad adds the goals of *possession*, *authenticity*, and *utility* (Parker, 2002, 2010), while goals proposed by others include *accuracy*, *completeness*, *consistency*, *non-repudiation*, *relevance*, and *timeliness* (Dardick, 2010).

Ways in Which Futuristic Neuroprostheses Challenge Traditional InfoSec Assumptions

In themselves, such developments suggest that neuroprosthetics researchers should no longer presume that the CIA Triad offers an appropriate starting point for exploring InfoSec for neuroprostheses. However, we would suggest two further reasons why the Triad provides an obsolete (and potentially even harmful) basis for analyzing InfoSec for futuristic neuroprostheses. Namely, some future neuroprostheses can be expected to violate the Triad's implicit assumptions that (1) computational systems to be secured are ultimately nothing more than instruments for expressing the agency of their human users, and (2) computing devices are conceptually and practically separable from their human users. Insofar as future neuroprostheses break those conditions, any InfoSec regimes designed for them on the basis of the CIA Triad may lack some security mechanisms needed to fully protect devices and their users while simultaneously implementing other mechanisms that can prove detrimental. Below we consider these points further.

SECURING FUTURISTIC NEUROPROSTHESES THAT ARE MORE THAN SIMPLY TOOLS

Classical InfoSec Frameworks' Instrumental Approach

The distinguishing feature of an "agent" is its possession of some degree of autonomous decision-making and action. Both human beings and artificial computing devices constitute agents, in different ways. The "strong" form of *biological agency* possessed by human beings is a complex amalgam of phenomena including conscious awareness; imagination; volition; conscience; rational decision-making influenced by emotion, instinct, and cognitive biases; and the embodiment of each mind within a unique physical form. This differs greatly from the "weak" form of *artificial agency* possessed by contemporary electronic computers, which possess a more limited and straightforward ability to process data and select a course of action without ongoing direct human control (Wooldridge and Jennings, 1995; Lind, 2001; Friedenberg, 2008; Fleischmann, 2009).

The CIA Triad arose in the 1970s as a practical aid for securing electronic computers that were processing increasingly sensitive and critical data. Built into the Triad is the historical assumption that an information system to be secured is not a biological agent but an expendable tool whose value subsists in the fact that it helps human users more effectively exercise their own biological agency by aiding them to process information, make decisions, and act for their own chosen ends. From that instrumental perspective, ensuring the confidentiality, integrity, and availability of information contained in a computer was considered sufficient to ensure the computer's adequate functioning as a tool for human use.

Most contemporary neuroprostheses are governed by computers constituting straightforward artificial agents, and the neuroprostheses themselves fill recognizable instrumental roles: for example, cochlear implants, retinal prostheses, and robotic prosthetic limbs allow human beings with certain medical conditions to perceive and manipulate their environment more effectively, while devices capable of detecting and interpreting a user's thoughts allow paralyzed but conscious patients to express their wishes (Merkel et al., 2007; McGee, 2008; Edlinger et al., 2011; Gasson et al., 2012; Lebedev, 2014).

Emerging Challenges to the Instrumental Vision of Neuroprostheses

The instrumental vision of technology presented above accepts the "neutrality thesis" that technological devices are created by human designers through the exercise of "instrumental rationality" and exist merely as passive tools that can be applied equally for either good or bad purposes. However, that view has been vigorously challenged as simplistic or wholly incorrect from various philosophical perspectives by thinkers like Heidegger, Marcuse, Ellul, Habermas, Virilio, Latour, and Fukuyama (Ellul, 1964; Habermas, 1970; Heidegger, 1977; Latour, 1996; Virilio, 1999; Marcuse, 2001, 2011; Fukuyama, 2002; Franssen et al., 2015).

Moreover, InfoSec's traditional instrumental model is expected to increasingly be undermined at the technological level by unconventional information systems like DNA-based and biological computers, physical (e.g., memristive) neural networks, nanorobotic swarms, evolvable software, self-improving robots, and hypothesized future forms of artificial general intelligence whose exercise of agency cannot necessarily be "programmed" or directly controlled by human beings for their own purposes (Friedenberg, 2008; Pearce, 2012; Yampolskiy and Fox, 2012; Gunkel, 2017). Insofar as future neuroprostheses incorporate such technologies, they may be less likely to simply support their hosts' biological agency; they might instead conceivably impair, override, transform, or replace it. This might be encountered, for example, with neuroprostheses that are controlled by computers possessing human-like cognitive abilities or are composed of biological components possessing their own biological agency distinct from that of their users (Rutten et al., 2007; Stieglitz, 2007; Gladden, 2016b).

Neuroprostheses' complex relationship to their users' agency is already revealed by existing devices. For example, it has been anecdotally noted that some users of deep brain stimulation implants report that their implants have strengthened their sense of autonomy and human agency: by treating disorders that had robbed them of motor control over their bodies, such devices have allowed their users to feel like "themselves" again for the first time in years. However, an opposite reaction has been anecdotally observed among other DBS users, who report that the devices undermine their sense of possessing full human agency, as they fear they can never entirely know which of their thoughts are truly "their own" and which might be generated by their implants (Kraemer, 2011; Van den Berg, 2012).

Futuristic Neuroprostheses' Intimate and Ambivalent Relationship with Human Agency

Futuristic neuroprostheses' relationship to their users' agency is expected to be even more fraught. For example, if researchers build on technologies already successfully tested in mice (Han et al., 2009; Josselyn, 2010; Ramirez et al., 2013) to develop neuroprostheses capable of interpreting, creating, altering, or erasing human beings' long-term memories, such devices might conceivably be used not only to treat phobias or aid with recovery from traumatic experiences (thereby enhancing patients' agency) but to alter or suppress memories of valued relationships, knowledge of moral principles, or the contents of firm decisions that an individual has already made—thereby impairing users' agency and replacing their judgment with that of the neuroprostheses' operators (Denning et al., 2009; Bonaci et al., 2015b).

The danger that neuroprostheses may not support their users' biological agency becomes more acute when considering the expected expansion of neuroprosthetics into the realm of human enhancement (Merkel et al., 2007; Gasson, 2008; McGee, 2008; Gasson et al., 2012). Future neuroprostheses may not be supplied by healthcare institutions interested solely in their patients' wellbeing but by military organizations deploying neuroprostheses to create more lethal augmented soldiers (Coker, 2004; Moreno, 2004; Kourany, 2014; Krishnan, 2015) or profit-oriented electronics firms seeking to offer computer gamers more immersive, thrilling, and potentially addictive VR experiences (Heidt, 1999; Kierkegaard, 2010; Scherer et al., 2012; Griffiths, 2017; Loup-Escande et al., 2017). It thus cannot be presumed—as the CIA Triad historically does—that enhancing the confidentiality, integrity, and availability of a device is equivalent to supporting the biological agency of its user. If ensuring such users' wellbeing is taken to be an important InfoSec aim, frameworks other than the CIA Triad will be needed to advance that goal.

HUMAN-MACHINE INTEGRATION: THE NEED TO SECURE THE BIOCYBERNETIC WHOLE

Historical InfoSec Assumptions That Computing Devices are Separable from their Users

Also implicit in the CIA Triad's goals is an understanding that information to be secured is contained in some artificial information system other than a human mind, like a web server or smartphone. InfoSec does address dangers like social engineering attacks that target human users; however, at a theoretical level the CIA Triad largely presumes that computing devices are structurally and operationally separable from their human users (Samonas and Coss, 2014). When the CIA Triad is employed to design protections for a conventional computer, it may thus yield mechanisms like anti-tamper casings, file backup systems, and antivirus software designed to secure the computer *as a device*, independently of whoever uses it.

The Neuroprosthetic Device and Its User as Elements of a Larger Biocybernetic System

It is expected, however, that future neuroprostheses may become structurally merged with their users' biological components and functionally integrated into their cognitive processes in powerful and intimate ways. Transdisciplinary research into futuristic neuroprostheses employing the tools of critical and philosophical posthumanism suggests that such devices may fuse with their human users through a process of "technological posthumanization" to create a qualitatively novel whole that is no longer simply a machine or a human being but a synthesis of the two possessing its own unique status (Hayles, 1999; Gray, 2002; Anderson, 2003; Clark, 2004; Herbrechter, 2013; Lilley, 2013; Naufel, 2013; Roden, 2014; Sandberg, 2014; Gladden, 2017). However, such analyses of the processes of "cyborgization" have had little impact on InfoSec, whose instrumental and technical perspective largely still views computers as tools easily separable from their human users.

Determining InfoSec Goals for the Whole Biocybernetic User-Device System

At a minimum, such analyses suggest that the CIA Triad might better be interpreted as requiring the confidentiality, integrity, and availability of information contained within the hybrid user-device system *as a whole*, rather than simply within its neuroprosthetic component. InfoSec mechanisms designed to protect information contained in a neuroprosthesis at all costs (e.g., by "failing closed" in case of a hardware problem) may endanger the safety and agency of its human host, while InfoSec practices that focus only on securing the biological elements of a user's organism may result in weak device security, thereby allowing devices to be compromised in ways that negatively impact their users. Such extremes of "subsystem optimization" can be prevented by keeping in mind the goal of optimizing InfoSec for the larger biocybernetic system formed through the coaction of a neuroprosthesis and its host. Because that whole *includes* a sapient human being possessing a unique legal and moral status (Wallach and Allen, 2008; Gunkel, 2012; Sandberg, 2014), technical issues become intertwined with complex social and philosophical questions.

At a deeper level, though, such analyses raise the question of whether a CIA Triad formulated decades ago for securing rudimentary electronic computers offers a viable starting point for developing robust InfoSec schemas for a human-computer whole. Indeed, it appears unlikely that human beings would spontaneously identify "confidentiality," "integrity," and "availability" of information as the most critical considerations for technologies that have such direct impacts on their own long-term psychological, physical, and social wellbeing (Denning et al., 2010; Bonaci et al., 2015b).

FROM DISCONNECTED GOALS TO A COHERENT AXIOLOGY OF INFOSEC VALUES FOR FUTURISTIC NEUROPROSTHESES

Futuristic neuroprostheses create many distinct layers of InfoSec concerns: for example, an immersive neuroprosthetic VR system that allows its user to stroll through a "virtual city" might not only threaten the integrity of the user's cerebral information system at the basic biological level by physically damaging his or her neurons; it could also distort that information system's contents at a higher semantic level by, for example, allowing the user to read "virtual newspapers" that contain blatantly false information.

With such challenges in mind, researchers have begun to informally identify a range of possible InfoSec goals relevant for futuristic neuroprostheses. As indicated in **Figure 1**, specialized InfoSec goals suggested for IMDs and their users include *device reliability; utility or usability; convenience; aesthetics; sensitivity to cultural and historical associations*; *acceptability to patients*; *adequate notification to users*; and *protection of users' safety, privacy, autonomy, psychological welfare, self-image, and public persona* (Halperin et al., 2008; Denning et al., 2010; Schechter, 2010; Clark and Fu, 2012). In the specific case of neuroprostheses, suggested InfoSec goals include *device reliability; ease of use; safety* (including *safety for users' neural mechanisms and computational processes*); the *distinguishability and rejectability of mental phenomena by users*; *protection of users' independence*, *free will, and human rights to privacy and dignity;* and *the autonomy of users and user-device systems* (Denning et al., 2009; Bonaci et al., 2015a,b; Gladden, 2016a).

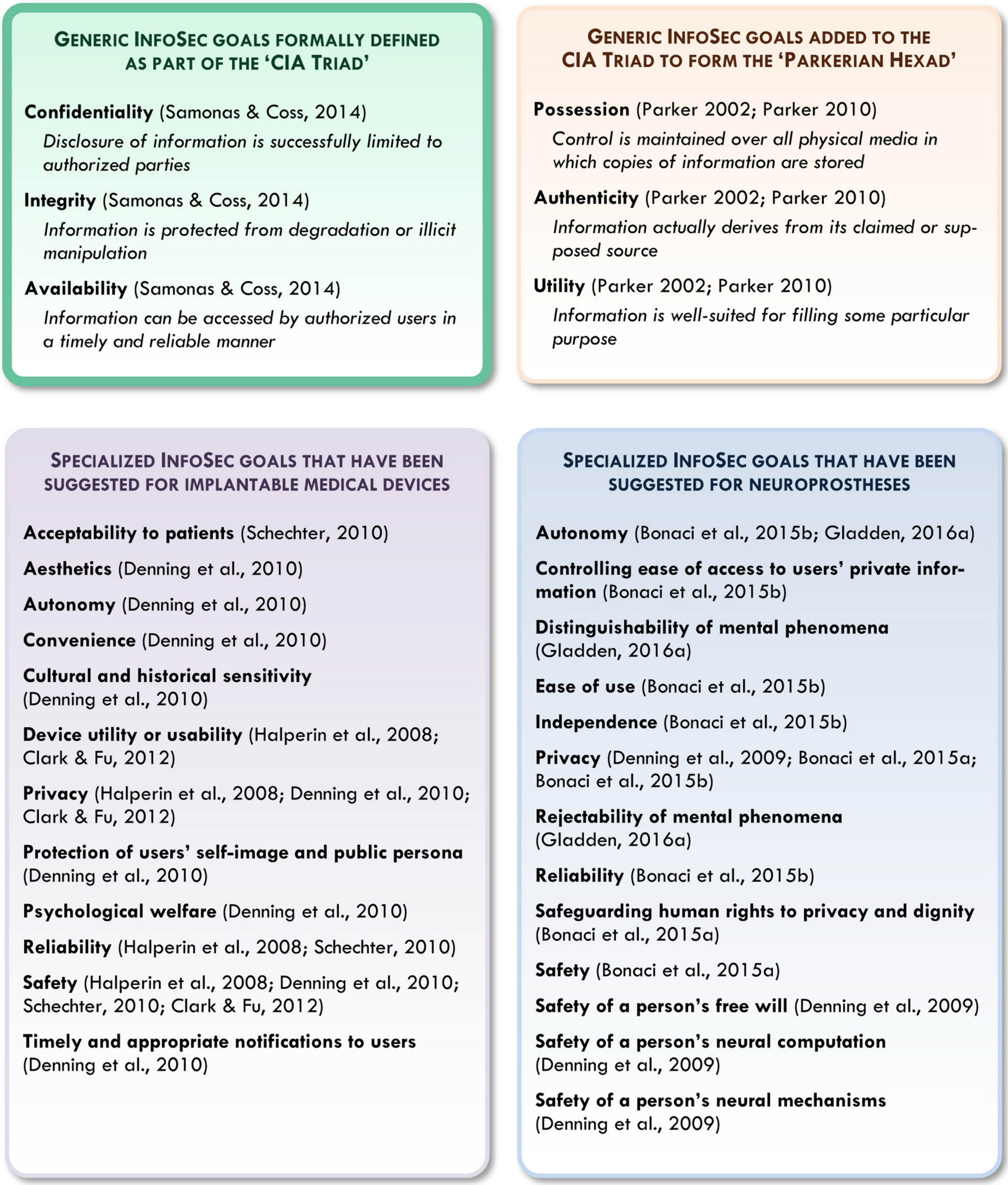
While some of these goals are directly ethical or legal in nature, others are primarily technical and technological—and still others (e.g., relating to convenience, cultural appropriateness, aesthetics, and a user's public persona) represent different sorts of aims that cannot be reduced simply to matters of law, ethics, or technical effectiveness. This suggests that InfoSec for futuristic neuroprostheses can be usefully analyzed through the lens of *axiology*, the philosophical investigation of values. Axiology encompasses not only ethics (with its consideration of actions that are right or wrong) but also aesthetics (with its investigation of goods like truth, harmony, and functionality) and the study of values associated with other types of goods.

Axiology allows us to identify, classify, understand, and prioritize goods in different ways. For example, some suggested InfoSec goals (like those relating to usability) might be understood as *instrumental goods*, which are valued because they allow us to achieve another desired end; other InfoSec goals (like those relating to safety and dignity) could be understood as intrinsic goods, which are valued in themselves because they are considered inherently worthwhile (Weber, 1978). InfoSec goals for neuroprostheses can also be classified according to whether they relate to ethical, aesthetic, physical (e.g., health-related), metaphysical, technological, psychological, historical, religious, economic, or social values (Hartman, 2011).

The information stored or processed by a neuroprosthesis reflects a complex tangle of such goods and values. For example, rich data regarding the functioning of a user's brain may possess not only *instrumental economic value* (e.g., if exploited by a device manufacturer) but also *intrinsic aesthetic value* (e.g., insofar as it reflects intricate biological patterns and elegant physical laws that manifest a certain natural beauty). Even superficial cosmetic aspects of a device can disclose significant information regarding the ethical, aesthetic, physical, technological, psychological, religious, economic, and social values held by its designer and user.

While there is much debate in the field of axiology surrounding such issues, there is broad agreement that, for example, in case of conflict, an *instrumental economic or technological good* (like that of ensuring a device's reliability or ease of use) should be given lower priority than an *intrinsic moral good* (like that of protecting users' safety or free will). As **Figure 2** suggests, superficially similar InfoSec goals may represent very different types of goods: safeguarding the availability of information in a neuroprosthesis may be an instrumental technological good, while safeguarding the availability of information in its user's mind might be an intrinsic moral and psychological good.

The exact nature of a neuroprosthesis also heavily influences which InfoSec issues and values will be relevant: for example, a



Generic InfoSec goals formally defined as part of the 'CIA Triad'

Confidentiality (Samonas & Coss, 2014)
Disclosure of information is successfully limited to authorized parties

Integrity (Samonas & Coss, 2014)
Information is protected from degradation or illicit manipulation

Availability (Samonas & Coss, 2014)
Information can be accessed by authorized users in a timely and reliable manner

Generic InfoSec goals added to the CIA Triad to form the 'Parkerian Hexad'

Possession (Parker 2002; Parker 2010)
Control is maintained over all physical media in which copies of information are stored

Authenticity (Parker 2002; Parker 2010)
Information actually derives from its claimed or supposed source

Utility (Parker 2002; Parker 2010)
Information is well-suited for filling some particular purpose

Specialized InfoSec goals that have been suggested for implantable medical devices

Acceptability to patients (Schechter, 2010)

Aesthetics (Denning et al., 2010)

Autonomy (Denning et al., 2010)

Convenience (Denning et al., 2010)

Cultural and historical sensitivity (Denning et al., 2010)

Device utility or usability (Halperin et al., 2008; Clark & Fu, 2012)

Privacy (Halperin et al., 2008; Denning et al., 2010; Clark & Fu, 2012)

Protection of users' self-image and public persona (Denning et al., 2010)

Psychological welfare (Denning et al., 2010)

Reliability (Halperin et al., 2008; Schechter, 2010)

Safety (Halperin et al., 2008; Denning et al., 2010; Schechter, 2010; Clark & Fu, 2012)

Timely and appropriate notifications to users (Denning et al., 2010)

Specialized InfoSec goals that have been suggested for neuroprostheses

Autonomy (Bonaci et al., 2015b; Gladden, 2016a)

Controlling ease of access to users' private information (Bonaci et al., 2015b)

Distinguishability of mental phenomena (Gladden, 2016a)

Ease of use (Bonaci et al., 2015b)

Independence (Bonaci et al., 2015b)

Privacy (Denning et al., 2009; Bonaci et al., 2015a; Bonaci et al., 2015b)

Rejectability of mental phenomena (Gladden, 2016a)

Reliability (Bonaci et al., 2015b)

Safeguarding human rights to privacy and dignity (Bonaci et al., 2015a)

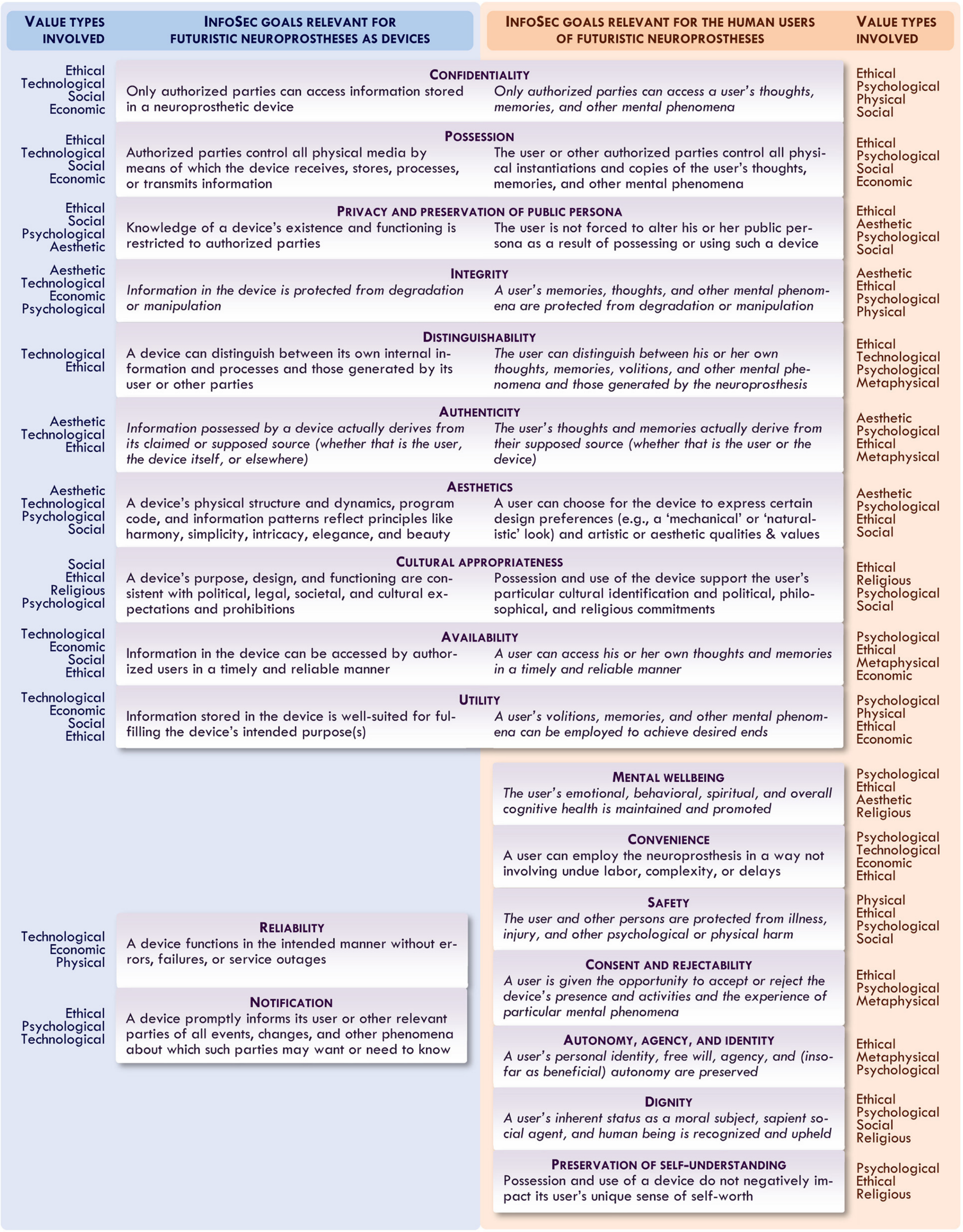
Safety (Bonaci et al., 2015a)

Safety of a person's free will (Denning et al., 2009)

Safety of a person's neural computation (Denning et al., 2009)

Safety of a person's neural mechanisms (Denning et al., 2009)

FIGURE 1 | A comparison of the generalized InfoSec goals formally defined in the CIA Triad and Parkerian Hexad with more specialized goals that have been suggested for implantable medical devices and neuroprostheses (including summaries or paraphrases of InfoSec goals that are discussed but not explicitly defined in their respective texts).



VALUE TYPES INVOLVED	INFOSEC GOAL	INFOSEC GOALS RELEVANT FOR FUTURISTIC NEUROPROSTHESES AS DEVICES	INFOSEC GOALS RELEVANT FOR THE HUMAN USERS OF FUTURISTIC NEUROPROSTHESES	VALUE TYPES INVOLVED
Ethical Technological Social Economic	CONFIDENTIALITY	Only authorized parties can access information stored in a neuroprosthetic device	*Only authorized parties can access a user's thoughts, memories, and other mental phenomena*	Ethical Psychological Physical Social
Ethical Technological Social Economic	POSSESSION	Authorized parties control all physical media by means of which the device receives, stores, processes, or transmits information	The user or other authorized parties control all physical instantiations and copies of the user's thoughts, memories, and other mental phenomena	Ethical Psychological Social Economic
Ethical Social Psychological Aesthetic	PRIVACY AND PRESERVATION OF PUBLIC PERSONA	Knowledge of a device's existence and functioning is restricted to authorized parties	The user is not forced to alter his or her public persona as a result of possessing or using such a device	Ethical Aesthetic Psychological Social
Aesthetic Technological Economic Psychological	INTEGRITY	*Information in the device is protected from degradation or manipulation*	*A user's memories, thoughts, and other mental phenomena are protected from degradation or manipulation*	Aesthetic Ethical Psychological Physical
Technological Ethical	DISTINGUISHABILITY	A device can distinguish between its own internal information and processes and those generated by its user or other parties	*The user can distinguish between his or her own thoughts, memories, volitions, and other mental phenomena and those generated by the neuroprosthesis*	Ethical Technological Psychological Metaphysical
Aesthetic Technological Ethical	AUTHENTICITY	*Information possessed by a device actually derives from its claimed or supposed source (whether that is the user, the device itself, or elsewhere)*	*The user's thoughts and memories actually derive from their supposed source (whether that is the user or the device)*	Aesthetic Psychological Ethical Metaphysical
Aesthetic Technological Psychological Social	AESTHETICS	A device's physical structure and dynamics, program code, and information patterns reflect principles like harmony, simplicity, intricacy, elegance, and beauty	A user can choose for the device to express certain design preferences (e.g., a 'mechanical' or 'naturalistic' look) and artistic or aesthetic qualities & values	Aesthetic Psychological Ethical Social
Social Ethical Religious Psychological	CULTURAL APPROPRIATENESS	A device's purpose, design, and functioning are consistent with political, legal, societal, and cultural expectations and prohibitions	Possession and use of the device support the user's particular cultural identification and political, philosophical, and religious commitments	Ethical Religious Psychological Social
Technological Economic Social Ethical	AVAILABILITY	Information in the device can be accessed by authorized users in a timely and reliable manner	*A user can access his or her own thoughts and memories in a timely and reliable manner*	Psychological Ethical Metaphysical Economic
Technological Economic Social Ethical	UTILITY	Information stored in the device is well-suited for fulfilling the device's intended purpose(s)	*A user's volitions, memories, and other mental phenomena can be employed to achieve desired ends*	Psychological Physical Ethical Economic
	MENTAL WELLBEING		*The user's emotional, behavioral, spiritual, and overall cognitive health is maintained and promoted*	Psychological Ethical Aesthetic Religious
	CONVENIENCE		A user can employ the neuroprosthesis in a way not involving undue labor, complexity, or delays	Psychological Technological Economic Ethical
	SAFETY		*The user and other persons are protected from illness, injury, and other psychological or physical harm*	Physical Ethical Psychological Social
Technological Economic Physical	RELIABILITY	A device functions in the intended manner without errors, failures, or service outages		
	CONSENT AND REJECTABILITY		*A user is given the opportunity to accept or reject the device's presence and activities and the experience of particular mental phenomena*	Ethical Psychological Metaphysical
Ethical Psychological Technological	NOTIFICATION	A device promptly informs its user or other relevant parties of all events, changes, and other phenomena about which such parties may want or need to know		
	AUTONOMY, AGENCY, AND IDENTITY		*A user's personal identity, free will, agency, and (insofar as beneficial) autonomy are preserved*	Ethical Metaphysical Psychological
	DIGNITY		*A user's inherent status as a moral subject, sapient social agent, and human being is recognized and upheld*	Ethical Psychological Social Religious
	PRESERVATION OF SELF-UNDERSTANDING		Possession and use of a device do not negatively impact its user's unique sense of self-worth	Psychological Ethical Religious

FIGURE 2 | A proposed axiological framework for analyzing InfoSec goals for futuristic neuroprostheses that are relevant particularly for devices (left) and their users (right); in the margins are noted values (ethical, psychological, physical, etc.) especially associated with a given InfoSec goal. Goals described in italics are those more likely to be recognized as intrinsic goods from some axiological perspectives.

noninvasive wearable visual neuroprosthesis, retinal implant, and visuocortical implant relate to the mind and body in different ways and raise very different issues. Many insights might be gained from the substantial existing body of axiological research regarding futuristic autonomous robots—especially since many futuristic neuroprostheses meet the definition of a specialized type of "robot" (Murphy, 2000; Bekey, 2005; Wallach and Allen, 2008; Gunkel, 2012).

CONCLUSION

In this text we have argued that as long as increasingly outdated instrumental schemas like the CIA Triad remain the default or "best" definition of InfoSec goals available to neuroprosthetics researchers, it will be difficult to develop InfoSec regimes for futuristic neuroprostheses that adequately address the complex issues they raise regarding human agency and human-machine integration. It is hoped that by formulating more robust axiological InfoSec frameworks of the sort sketched above—which look beyond instrumental approaches to consider the relationship of "information" and "information systems" to a wide range of values and goods—futuristic neuroprostheses and their users can be protected against dangers including not only conventional data theft or financial loss but also threats to the essential dynamics of memory, consciousness, conscience, and autonomy that lie at the heart of what makes us human.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and approved it for publication.

REFERENCES

Anderson, W. T. (2003). Augmentation, symbiosis, transcendence: technology and the future(s) of human identity. *Futures* 35, 535–546. doi: 10.1016/S0016-3287(02)00097-6

Bekey, G. A. (2005). *Autonomous Robots: From Biological Inspiration to Implementation and Control*. Cambridge, MA: MIT Press.

Bergamasco, S., Bon, M., and Inchingolo, P. (2001). "Medical data protection with a new generation of hardware authentication tokens," in *IFMBE Proceedings MEDICON 2001*, eds R. Magjarevic, S. Tonkovic, V. Bilas, and I. Lackovic (Zagreb: IFMBE), 82–85.

Bonaci, T. (2015). *Security and Privacy of Biomedical Cyber-Physical Systems*. Ph.D. dissertation, University of Washington.

Bonaci, T., Calo, R., and Chizeck, H. J. (2015a). App stores for the brain: privacy and security in brain-computer interfaces. *IEEE Technol. Soc. Magazine* 34, 32–39. doi: 10.1109/MTS.2015.2425551

Bonaci, T., Herron, J., Matlack, C., and Chizeck, H. J. (2015b). Securing the exocortex: a twenty-first century cybernetics challenge. *IEEE Technol. Soc. Magazine* 34, 44–51. doi: 10.1109/MTS.2015.2461152

Cho, K., and Lee, D. H. (2012). "Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks," in *Information Security Applications*, eds S. Jung and M. Yung (Berlin; Heidelberg: Springer), 203–218.

Clark, A. (2004). *Natural-born Cyborgs: Minds, Technologies, and the Future of Human Intelligence*. Oxford: Oxford University Press.

Clark, S. S., and Fu, K. (2012). "Recent results in computer security for medical devices," in *Wireless Mobile Communication and Healthcare*, eds K. S. Nikita, J. C. Lin, D. I. Fotiadis, and M.-T. Arredondo Waldmeyer (Berlin; Heidelberg: Springer), 111–18.

Coker, C. (2004). Biotechnology and war: the new challenge. *Aust. Army J.* 2, 125–140.

Dardick, G. (2010). "Cyber forensics assurance," in *Proceedings of the 8th Australian Digital Forensics Conference* (Perth: SecAU Security Research Centre), 57–64.

Denning, T., Borning, A., Friedman, B., Gill, B. T., Kohno, T., and Maisel, W. H. (2010). "Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY: ACM), 917–926.

Denning, T., Fu, K., and Kohno, T. (2008). "Absence makes the heart grow fonder: new directions for implantable medical device security," in *3rd USENIX Workshop on Hot Topics in Security (HotSec 2008)* (San Jose, CA), 29.

Denning, T., Matsuoka, Y., and Kohno, T. (2009). Neurosecurity: security and privacy for neural devices. *Neurosurgical. Focus* 27:E7. doi: 10.3171/2009.4.FOCUS0985

Edlinger, G., Rizzo, C., and Guger, C. (2011). "Brain computer interface," in *Springer Handbook of Medical Technology*, eds R. Kramme, K.-P. Hoffmann, and R. S. Pozos (Berlin; Heidelberg: Springer), 1003–1017.

Ellul, J. (1964). *The Technological Society*. Trans. J. Wilkinson. New York, NY: Vintage Books.

Fleischmann, K. R. (2009). Sociotechnical interaction and cyborg–cyborg interaction: transforming the scale and convergence of HCI. *Inform. Soc.* 25, 4, 227–235. doi: 10.1080/01972240903028359

Franssen, M., Lokhorst, G.-J., and Van de Poel, I. (2015). "Philosophy of Technology," in *The Stanford Encyclopedia of Philosophy*, ed E. N. Zalta. Available online at: https://plato.stanford.edu/archives/fall2015/entries/technology/ (Accessed October 12, 2017).

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

Friedenberg, J. (2008). *Artificial Psychology: The Quest for What It Means to Be Human*. Philadelphia, PA: Psychology Press.

Fukuyama, F. (2002). *Our Posthuman Future: Consequences of the Biotechnology Revolution*. New York, NY: Farrar, Straus, and Giroux.

Gasson, M. N. (2008). "ICT implants," in *The Future of Identity in the Information Society*, eds S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci (Boston, MA: Springer), 287–295. doi: 10.1007/978-0-387-79026-8_20

Gasson, M. N., Kosta, E., and Bowman, D. M. (2012). "Human ICT implants: from invasive to pervasive," in *Human ICT Implants: Technical, Legal and Ethical Considerations*, eds M. N. Gasson, E. Kosta, and D. M. Bowman (The Hague: T. M. C. Asser Press), 1–8.

Gladden, M. E. (2016a). "Information security concerns as a catalyst for the development of implantable cognitive neuroprostheses," in *Proceedings of the 9th Annual EuroMed Academy of Business Conference: Innovation, Entrepreneurship and Digital Ecosystems (EUROMED 2016)*, eds D. Vrontis, Y. Weber, and E. Tsoukatos (Engomi: EuroMed Press), 891–904.

Gladden, M. E. (2016b). "Neural implants as gateways to digital-physical ecosystems and posthuman socioeconomic interaction," in *Digital Ecosystems: Society in the Digital Age*, eds Ł. Jonak, N. Juchniewicz, and R. Włoch (Warsaw: Digital Economy Lab, University of Warsaw), 85–98.

Gladden, M. E. (2017). *The Handbook of Information Security for Advanced Neuroprosthetics, 2nd Edn*. Indianapolis, IN: Synthypnion Academic.

Gray, C. H. (2002). *Cyborg Citizen: Politics in the Posthuman Age*. London: Routledge.

Griffiths, M. (2017). The psychosocial impact of gambling in virtual reality. *Casino Gaming Int.* 29, 51–54.

Gunkel, D. J. (2012). *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*. Cambridge, MA: The MIT Press.

Gunkel, D. J. (2017). Mind the gap: responsible robotics and the problem of responsibility. *Ethics Inform. Technol.* doi: 10.1007/s10676-017-9428-2. [Epub ahead of print].

Habermas, J. (1970). *Toward A Rational Society*. Trans. J. J. Shapiro. Boston, MA: Beacon.

Halperin, D., Kohno, T., Heydt-Benjamin, T. S., Fu, K., and Maisel, W. H. (2008). Security and privacy for implantable medical devices. *IEEE Pervasive Comput.* 7, 30–39. doi: 10.1109/MPRV.2008.16

Han, J.-H., Kushner, S. A., Yiu, A. P., Hsiang, H.-W., Buch, T., Waisman, A., et al. (2009). Selective erasure of a fear memory. *Science* 323, 1492–1496. doi: 10.1126/science.1164139

Hansen, J. A., and Hansen, N. M. (2010). "A taxonomy of vulnerabilities in implantable medical devices," in *Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-Care Systems* (New York, NY: ACM), 13–20. doi: 10.1145/1866914.1866917

Hartman, R. S. (2011). *The Structure of Value: Foundations of Scientific Axiology*. Eugene, OR: Wipf and Stock Publishers.

Hayles, N. K. (1999). *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago, IL: University of Chicago Press.

Hei, X., and Du, X. (2011). "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proceedings of IEEE INFOCOM 2011* (Piscataway, NJ: IEEE), 346–350. doi: 10.1109/INFCOM.2011.5935179

Heidegger, M. (1977). *The Question Concerning Technology and Other Essays*. Trans. W. Lovitt. New York, NY: Garland Publishing, Inc.

Heidt, S. (1999). Floating, flying, falling: a philosophical investigation of virtual reality technology. *Inquiry* 18, 77–98. doi: 10.5840/inquiryctnews19991846

Herbrechter, S. (2013). *Posthumanism: A Critical Analysis*. London: Bloomsbury.

Josselyn, S. A. (2010). Continuing the search for the engram: examining the mechanism of fear memories. *J. Psychiatry Neurosci.* 35, 221–228. doi: 10.1503/jpn.100015

Kierkegaard, P. (2010). The brain as game controller. *Int. J. Liability Sci. Enq.* 3, 165–177. doi: 10.1504/IJLSE.2010.031831

Kourany, J. A. (2014). Human enhancement: making the debate more productive. *Erkenntnis* 79, 981–998. doi: 10.1007/s10670-013-9539-z

Kraemer, F. (2011). Me, myself and my brain implant: deep brain stimulation raises questions of personal authenticity and alienation. *Neuroethics* 6, 483–497. doi: 10.1007/s12152-011-9115-7

Krishnan, A. (2015). "Enhanced warfighters as private military contractors," in *Super Soldiers: The Ethical, Legal and Social Implications*, eds J. Galliott and M. Lotz (London: Routledge), 65–80.

Latour, B. (1996). *Aramis, Or the Love of Technology*. Cambridge, MA: Harvard University Press.

Lebedev, M. (2014). Brain-machine interfaces: an overview. *Transl. Neurosci.* 5, 99–110. doi: 10.2478/s13380-014-0212-z

Lilley, S. (2013). *Transhumanism and Society: The Social Debate Over Human Enhancement*. Dordrecht: Springer Science and Business Media.

Lind, J. (2001). "Issues in agent-oriented software engineering," in *Agent-Oriented Software Engineering*, eds P. Ciancarini and M. J. Wooldridge (Berlin; Heidelberg: Springer), 45–58.

Loup-Escande, E., Lotte, F., Loup, G., and Lécuyer, A. (2017). "User-centered BCI videogame design," in *Handbook of Digital Games and Entertainment Technologies*, eds R. Nakatsu, M. Rauterberg, and P. Ciancarini (Singapore: Springer), 225–250. doi: 10.1007/978-981-4560-50-4_3

Marcuse, H. (2001). "The problem of social change in the technological society," in *Towards a Critical Theory of Society*, ed D. Kellner (London: Routledge Press), 35–58.

Marcuse, H. (2011). "From ontology to technology," in *Philosophy, Psychoanalysis and Emancipation*, ed D. Kellner (London: Routledge Press), 132–140.

McGee, E. M. (2008). "Bioelectronics and implanted devices," in *Medical Enhancement and Posthumanity*, eds B. Gordijn and R. Chadwick (Dordrecht: Springer), 207–224.

Merkel, R., Boer, G., Fegert, J., Galert, T., Hartmann, D., Nuttin, B., et al. (2007). "Central neural prostheses," in *Intervening in the Brain: Changing Psyche and Society, Ethics of Science and Technology Assessment 29* (Berlin; Heidelberg: Springer), 117–160.

Moreno, J. (2004). DARPA on your mind. *Cerebrum* 6, 92–100.

Murphy, R. (2000). *Introduction to AI Robotics*. Cambridge, MA: The MIT Press.

Naufel, S. (2013). "Nanotechnology, the brain, and personal identity," in *Nanotechnology, the Brain, and the Future*, eds S. A. Hays, J. S. Robert, C. A. Miller, and I. Bennett (Dordrecht: Springer Science+Business Media), 167–178.

Parker, D. (2002). "Toward a new framework for information security," in *The Computer Security Handbook, 4th Edn.*, eds S. Bosworth and M. E. Kabay (New York, NY: John Wiley & Sons), 5.1–5.21.

Parker, D. (2010). Our excessively simplistic information security model and how to fix it. *ISSA J.* 8, 12–21.

Pearce, D. (2012). "The biointelligence explosion," in *Singularity Hypotheses*, eds A. H. Eden, J. H. Moor, J. H. Søraker, and E. Steinhart (Berlin; Heidelberg: Springer), 199–238.

Ramirez, S., Liu, X., Lin, P.-A., Suh, J., Pignatelli, M., Redondo, R. L., et al. (2013). Creating a false memory in the hippocampus. *Science* 341, 387–391. doi: 10.1126/science.1239073

Rasmussen, K. B., Castelluccia, C., Heydt-Benjamin, T. S., and Capkun, S. (2009). "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM Conference on Computer and Communications Security* (New York, NY: ACM), 410–419.

Roden, D. (2014). *Posthuman Life: Philosophy at the Edge of the Human*. Abingdon: Routledge.

Rotter, P., and Gasson, M. N. (2012). "Implantable medical devices: privacy and security concerns," in *Human ICT Implants: Technical, Legal and Ethical Considerations*, eds M. N. Gasson, E. Kosta, and D. M. Bowman (The Hague: T. M. C. Asser Press), 63–66. doi: 10.1007/978-90-6704-870-5_6

Rutten, W. L., Ruardij, T. G., Marani, E., and Roelofsen, B. H. (2007). "Neural networks on chemically patterned electrode arrays: towards a cultured probe," in *Operative Neuromodulation*, *Vol. 2*, eds D. E. Sakas and B. A. Simpson (Vienna: Springer), 547–554.

Samonas, S., and Coss, D. (2014). The CIA strikes back: redefining confidentiality, integrity and availability in security. *J. Inform. Syst. Security* 10, 21–45.

Sandberg, A. (2014). Ethics of brain emulations. *J. Exp. Theor. Arti. Intelligence* 26, 439–457. doi: 10.1080/0952813X.2014.895113

Schechter, S. (2010). *Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices*. Microsoft Research. Available online at: https://www.microsoft.com/en-us/research/publication/security-that-is-meant-to-be-skin-deep-using-ultraviolet-micropigmentation-to-store-emergency-access-keys-for-implantable-medical-devices/ (Accessed on July 26, 2015).

Scherer, R., Pröll, M., Allison, B., and Müller-Putz, G. R. (2012). "New input modalities for modern game design and virtual embodiment," in *2012 IEEE Virtual Reality Short Papers and Posters (VRW)* (Piscataway, NJ: IEEE), 163–164.

Stieglitz, T. (2007). "Restoration of neurological functions by neuroprosthetic technologies: future prospects and trends towards micro-, nano-, and biohybrid systems," in *Operative Neuromodulation*, Vol. 1, eds D. E. Sakas, B. A. Simpson, and E. S. Krames (Vienna: Springer), 435–442.

Van den Berg, B. (2012). "Pieces of Me: on identity and information and communications technology implants," in *Human ICT Implants: Technical, Legal and Ethical Considerations*, eds M. N. Gasson, E. Kosta, and D. M. Bowman (The Hague: T. M. C. Asser Press), 159–173.

Virilio, P. (1999). *Politics of the Very Worst*. Trans. M. Cavaliere. New York, NY: Semiotext(e).

Wallach, W., and Allen, C. (2008). *Moral Machines: Teaching Robots Right from Wrong*. New York, NY: Oxford University Press.

Weber, M. (1978). *Economy and Society.* eds G. Roth and C. Wittich. Berkeley, CA: University of California Press.

Wooldridge, M., and Jennings, N. R. (1995). "Intelligent agents: theory and practice." *Knowledge Engin. Rev.* 10, 115–152. doi: 10.1017/S0269888900008122

Yampolskiy, R. V., and Fox, J. (2012). "Artificial general intelligence and the human mental model," in *Singularity Hypotheses*, eds A. H. Eden, J. H. Moor, J. H. Søraker, and E. Steinhart (Berlin; Heidelberg: Springer), 129–145.

Zheng, G., Fang, G., Orgun, M., and Shankaran, R. (2014). "A non-key based security scheme supporting emergency treatment of wireless implants," in *2014 IEEE International Conference on Communications (ICC)* (Piscataway, NJ: IEEE), 647–652.

Conflict of Interest Statement: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.