*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

## Chapter Four

# An Information Security Device Ontology for Advanced Neuroprosthetics

## Introduction to the ontology

In order to create an effective information security framework for neuroprosthetics, it is necessary to first develop an appropriate ontology for such devices. Such an ontology should define the range of possible values for relevant characteristics that are critical for information security and whose values can vary across the universe of neuroprosthetic devices. The ontology should include both the physical characteristics, processes, and contexts and relationships possessed by such devices; it thus differs from (and is necessary for the effective development of) security configuration checklists[1] that would be used to configure particular neuroprosthetic devices for secure operation in their individual human hosts.

Scholars and device manufacturers have made efforts to create general ontologies for robotic systems[2] and mobile devices,[3] however there has not yet been developed an ontology that focuses on the information security characteristics of neuroprosthetic devices. In part, the lack of creation of such formal tools is an effect of the relatively low level of interaction and collaboration between the fields of information security and biomedical engineering.[4]

By synthesizing information gathered from a review of current literature and practice in the fields of neuroprosthetics, implantable computing, and information security, we develop one such ontology within this chapter. Note that because many neuroprosthetic devices are also computers, mobile devices, or implantable medical devices, any generalized information security ontology that is applicable to computers, mobile devices, or IMDs will also

---

[1] *NIST SP 800-70, Rev. 2* (2011).

[2] See Prestes et al., "Towards a Core Ontology for Robotics and Automation" (2013).

[3] See "FIPA Device Ontology Specification" (2002).

[4] See Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

apply to the relevant kinds of neuroprosthetic devices. The specialized ontology developed here can be understood as a more detailed and focused extension and complement to such ontologies that analyzes the form and functioning of neuroprosthetic devices from the perspective of their particular information security features and risks.

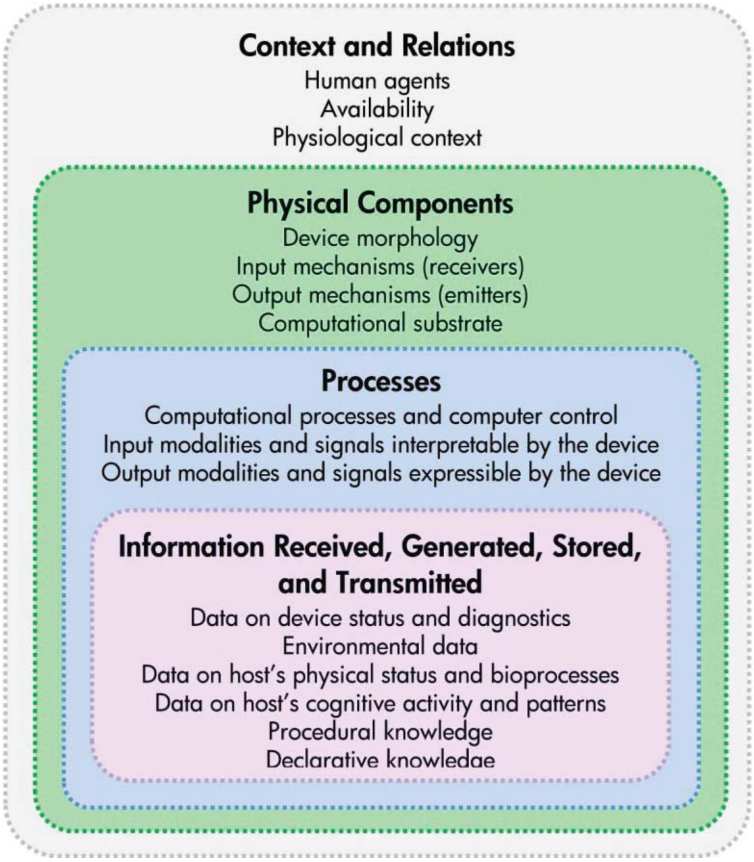

*Figure 1. The four main areas constituting the information security device ontology for advanced neuroprosthetics, along with the particular variables taken into account within each area.*

As is illustrated in Figure 1 above, our ontology is organized into four areas. It categorizes neuroprosthetic devices according to: 1) their context and rela-

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

tions; 2) their physical components; 3) their processes; and 4) the data, information, and knowledge that is received, stored, and transmitted by the devices.

Each area comprises a number of individual characteristics which we address in detail in the following sections. Together, a device's values for these variables comprise the information security profile for that particular neuroprosthetic device. The ontology presumes that a neuroprosthetic device is an implantable unit, but it can also be applied to nonimplantable external systems (in which case a few of the specific characteristics may not be relevant).

## First area: context and relations

This part of the ontology describes the physical, socioeconomic, and political context in which a neuroprosthetic device is being employed. This context helps determine which individuals have access to the device and for what purposes it may be used. Specific characteristics in this area are:

### Human agents

The human agents[5] who are in different ways responsible for a neuroprosthetic device's functioning include its:

- **Designer**,[6] who determines the basic parameters for the device's form and functioning.
- **Manufacturer**, which physically implements the neuroprosthetic device's design and controls its wholesale distribution[7] and which likely has a unique history of past information security practices, product security flaws, and responses to those flaws.[8]
- **Regulators**,[9] who exercise legal and political power within local, national, or international bodies, who may require or forbid that the device possess certain physical components, processes, or functions, and who may mandate or restrict its distribution and use for certain classes

---

[5] On the impact of such human agents, see Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

[6] Regarding the importance of a device's designer, see Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012), and McCullagh et al., "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology" (2013).

[7] For a device ontology that incorporates manufacturer information, see "FIPA Device Ontology Specification" (2002).

[8] See *NIST SP 800-100* (2006).

[9] On the role of regulators and regulation, see McCullagh et al., "Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology" (2013); Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008); and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

of users. Multiple jurisdictions may be involved, since a neuroprosthetic device's human host can travel between and within geographically dispersed locations and devices can potentially transmit data to or be controlled from remote locations that are distant from the site at which the device and its user are currently located.

- **Owner**, who owns the physical device but may or may not be the host in whom the device is implanted and may or may not own the rights to intellectual property that is produced by or stored in it. If a device is leased to a user rather than sold, the device's manufacturer or an intermediary firm leasing it to the end user may remain the device's owner.
- **Host** in whose body the neuroprosthetic device has been temporarily or permanently implanted. Depending on the nature of the device, the host may or may not realize that it has been implanted[10] and may or may not have an ability to consciously control or exploit the device's functioning. A host could potentially contribute to or actively undermine the secure functioning of a device.[11]
- **User** (or **operator**) who has the ability to monitor and consciously control or exploit the device's functioning.[12] In the case of neuroprosthetic devices, the operator might collectively be the medical staff in a hospital who remotely monitor and control the device's operation, rather than the human host in whose body the device has been implanted.[13]

---

[10] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[11] For psychological, social, and cultural factors that might cause the host of an implanted device to intentionally ignore, disable, or otherwise subvert a device's security features and mechanisms – despite the host's awareness that this might put him or her at greater risk of harm – see Denning et al., "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices" (2010).

[12] See *NIST SP 800-100* (2006) and Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012). For the extent to which the organizational culture and constraints of a device's operator can affect information security, see Cavallari, "Organisational Constraints on Information Systems Security" (2011). For ways in which power relationships between, e.g., the owner, host, and operator of a device might affect compliance with information security policies and procedures that have been developed by one or more of the parties, see Kolkowska & Dhillon, "Organizational Power and Information Security Rule Compliance" (2011).

[13] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012). While the use of remotely controlled implantable devices creates the possibility of illicit surveillance of a device's human host by medical personnel, such remote monitoring may also have positive effects – e.g., making it easier to gather needed medical data from individuals who consider implanted devices less bothersome than external systems; see Lorence et al., "Transac-

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

A military unit may be the operator of devices implanted in military personnel. A governmental intelligence agency, corporate business intelligence offices, or cybercriminals may be the operators of devices that were implanted (or have been hijacked) for use in surveillance, intelligence-gathering, or espionage.

## Factors impacting availability

Factors determining the extent to which a neuroprosthetic device (and its related external system components, replacement parts, software, and technical manuals) may be available for acquisition by intended or unintended users include its:

- **Licensing and legality**,[14] which may ban certain kinds of neuroprosthetic devices altogether and require medical certification for those implanting other kinds of neuroprosthetics and medical prescriptions for their hosts.
- **Cost**, which may place significant practical limits on the ability of individuals or organizations to acquire neuroprosthetic devices or their components or maintenance equipment.[15]
- **Required expertise**[16] that is needed to acquire, implant, and operate neuroprosthetic devices may significantly limit their potential use.[17]
- **Required maintenance**[18] may restrict use of devices to institutions or individuals that possess appropriate maintenance facilities and supply chains.
- **Required user customization**[19] may limit devices' availability, if a device must be extensively customized for each host or user – whether

---

tion-Neutral Implanted Data Collection Interface as EMR Driver: A Model for Emerging Distributed Medical Technologies" (2009). Implantable devices can allow remote care for those in underserved remote areas and potentially increase efficiency while decreasing cost and aggravations associated with in-hospital care; see Reynolds et al., "Device Therapy for Remote Patient Management" (2008).

[14] See McGee, "Bioelectronics and Implanted Devices" (2008), and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants" (2012).

[15] See McGee, "Bioelectronics and Implanted Devices" (2008), and Park et al., "The Future of Neural Interface Technology" (2009).

[16] See Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012), and Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[17] For issues relating to the training of users of BCI systems, see Neuper & Pfurtscheller, "Neurofeedback Training for BCI Control" (2009).

[18] See *NIST SP 800-100* (2006).

[19] See Merkel et al., "Central Neural Prostheses" (2007); Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); and Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

through physical fittings of prosthetics, adaptation of device software to a host's unique neurological or behavioral characteristics, or assurance of biological and genetic compatibility (for devices with organic components[20]). Similarly, the ability to use devices may be limited if the anatomical structures, biological processes, or psychological activity of potential hosts or users must be "customized" prior to or after implantation in order to allow operation of the device.

- **Reusability** of a device, which can increase the availability of previously implanted neuroprosthetic devices and require effective procedures for the disposal of devices after use in order to ensure information security.[21]

## Physiological context

The relevant aspects of an implantable neuroprosthetic device's context and situation within its host's body include the:

- **Lifespan** that the device is expected to demonstrate[22] before it requires replacement[23] or invasive maintenance.
- **Physical situation in the body**, which includes the neuroprosthetic device's specific location within the host's body and its physical connections to bodily organs and which also affects the device's:
    - **Physical visibility and discoverability**[24] to both the human host and other human beings interacting with the host.
    - **Physical access to alter the device**,[25] as the fact that a neuroprosthetic device is visibly present does not necessarily entail the possibility of physically accessing the device's key components.
    - **Remote discoverability**, the ability of external devices such as X-ray scanners, millimeter wave scanners, Wi-Fi routers, or Bluetooth

---

[20] See Merkel et al., "Central Neural Prostheses" (2007).

[21] See *NIST SP 800-100* (2006).

[22] See Merkel et al., "Central Neural Prostheses" (2007).

[23] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[24] See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

[25] See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.

devices to identify and localize the neuroprosthetic device from outside of its host's body, even when the device is not visible.[26]

- **Level of neurocognitive interface** between the neuroprosthetic device and the conscious awareness and unconscious cognitive activities of its human host.[27] This includes the extent to which the device's host (who may be different from its primary user) is consciously aware[28] of the device's presence, status, and activity, and the extent to which the device's functioning is determined by the host's neural activity. For example, devices serving as part of an input neural interface system might electrically stimulate afferent neurons to provide sense data to their human host,[29] while mnemoprosthetic devices might interact with interneurons in the host's brain to participate in processes of memory encoding, storage, and retrieval.
- **Health sensitivity and criticality**. A neuroprosthetic device that can directly affect, for example, the functioning of its host's heart or brain requires more safeguards than one that has no such capacity.

## Second area: physical components

This part of the ontology describes the key physical components of the neuroprosthetic device that have implications for information security. Specific characteristics of this area are:

### Device morphology

The device's basic physical morphology includes its:

- **Identity and unitarity**, which describe whether the neuroprosthetic device is a single, clearly identifiable physical unit, or whether the device comprises a large number of small physical components (such as a nanorobot swarm[30]) whose nature and location cannot easily be identified.
- **Size**[31] of the neuroprosthetic device (whether a unit implanted within the host's body or an external unit).

---

[26] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[27] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); "FIPA Device Ontology Specification" (2002); and Merkel et al., "Central Neural Prostheses" (2007).

[28] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[29] See Park et al., "The Future of Neural Interface Technology" (2009).

[30] See McGee, "Bioelectronics and Implanted Devices" (2008).

[31] See "FIPA Device Ontology Specification" (2002).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

- **Materials** from which the device is constructed.[32] While some neuroprosthetic devices may be wholly electromechanical devices, others may include organic (and perhaps even living[33]) components.
- **System participation**.[34] While some neuroprosthetic devices might function as standalone devices, others may simply be the implanted portion of a larger system that also includes monitoring and control equipment outside of the host's body[35] or external actuators or other components (or even entire external systems, such as an exoskeleton, vehicle, or 3D printer) that are remotely controlled by the neuroprosthetic device.[36] Multiple implanted neuroprosthetic devices may also interact to form an implanted body area network (BAN).[37]

## Input mechanisms: physical receivers of matter, energy, and information

A neuroprosthetic device's physical mechanisms for receiving input in the form of matter, energy, or information[38] may include:

- **A power supply**.[39] Important are both the nature of the device's primary power source (whether an internal battery, external wireless or wired power supply, or power supplied by the host's organism), the ability to utilize any backup or alternative power sources, and the behavior that the device will demonstrate if its primary (or only) supply of power is lost.
- **Physical ports and controls** such as on/off switches, microSD card slots, or micro-USB or proprietary communication ports.[40]

---

[32] See McGee, "Bioelectronics and Implanted Devices" (2008).

[33] See Merkel et al., "Central Neural Prostheses" (2007).

[34] See Prestes et al., "Towards a Core Ontology for Robotics and Automation" (2013), and *NIST SP 800-100* (2006).

[35] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), and Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009).

[36] See Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

[37] See Sayrafian-Pour et al., "Channel Models for Medical Implant Communication" (2010).

[38] See "FIPA Device Ontology Specification" (2002).

[39] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Merkel et al., "Central Neural Prostheses" (2007); and Li et al., "Advances and Challenges in Body Area Network" (2011).

[40] See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

- **Environmental sensors** through which the neuroprosthetic device receives input from the environment outside of its host's body. This may include:
    - **Specialized data reception mechanisms**[41] such as photoreceptors, ultrasonic sensors,[42] or radio receivers that are intentionally designed to detect particular signals for processing by the device.
    - **Unpurposeful receptors** in the form of components that were not designed to function as sensors but which can nevertheless be affected by environmental phenomena (such as electromagnetic radiation, heat, or acceleration). Many, if not all, of a device's components will be unpurposeful receptors (in addition to whatever other roles they might fill), insofar as their structure or performance can be affected by external forces or phenomena.
- **Neuronal input mechanisms**[43] through which the device receives electrochemical signals from either afferent neurons, efferent neurons, or interneurons within the host's body, potentially through a brain-computer interface (BCI).[44] Input can come from a large group of neurons or a single neuron.[45]

### Output mechanisms: physical emitters of matter, energy, and information

The device's physical mechanisms for generating output in the form of matter, energy, or information may include:[46]

---

[41] See "FIPA Device Ontology Specification" (2002); Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Park et al., "The Future of Neural Interface Technology" (2009); Merkel et al., "Central Neural Prostheses" (2007); and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[42] See Warwick & Gasson, "Implantable Computing" (2008).

[43] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010), and Park et al., "The Future of Neural Interface Technology" (2009).

[44] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Merkel et al., "Central Neural Prostheses" (2007).

[45] Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010), and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[46] See "FIPA Device Ontology Specification" (2002), pp. 6-8, for an example of how such mechanisms could be described and categorized

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

- **Physical actuators** such as robotic prostheses that are controlled by the neuroprosthetic device.[47] Speakers used to broadcast synthesized speech[48] are also, in a sense, highly specialized actuators.
- **Environmental emitters** through which the neuroprosthetic device affects the environment outside of its host's body.[49] This may include:
    - **Specialized data transmission mechanisms**[50] such as radio,[51] optical, and ultrasonic transmitters and electromagnetic induction mechanisms that have been intentionally designed.[52]
    - **Unpurposeful emitters** in the form of components that were not designed to function as transmitters but which can nevertheless affect the external environment (e.g., by producing audible sounds or electromagnetic radiation).
- **Neuronal output mechanisms**[53] through which the device transmits electrochemical signals to either afferent neurons, efferent neurons, or interneurons within the host's body, potentially through a BCI.[54]

## Computational substrate

In their role as computers, some neuroprosthetic devices may display a physical computational architecture based on the execution of programs by a serial processor; others may take the form of a physical neural network that

---

[47] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); Merkel et al., "Central Neural Prostheses" (2007); Lebedev, "Brain-Machine Interfaces: An Overview" (2014); and Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

[48] See Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008).

[49] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[50] See "FIPA Device Ontology Specification" (2002) and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[51] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[52] Regarding the importance of reliable data-transport systems for transmitting data from an implanted device to other implanted devices or external systems, see Fernandez-Lopez et al., "The Need for Standardized Tests to Evaluate the Reliability of Data Transport in Wireless Medical Systems" (2012).

[53] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); and Park et al., "The Future of Neural Interface Technology" (2009).

[54] See Merkel et al., "Central Neural Prostheses" (2007).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

does not execute programs. An information security ontology should describe the specifications of a device's:

- **CPU-based systems**[55] (if applicable) which can be used to execute traditional software programs. These processing abilities are constrained by the characteristics of a system's:
  - **Processor(s)**, which might take the form of a single central processing unit (CPU),[56] a multicore computer, or a CPU-based cluster or grid.
  - **Memory**,[57] which might include volatile RAM used as primary storage, non-volatile RAM used as longer-term secondary storage, and non-volatile ROM used for storing firmware or data that should not be altered.
- **Physical neural networks** (if applicable) that comprise a large number of artificial neurons that transmit signals to one another through artificial synapses and which store data in the form of activation patterns within the networks. While capable of processing input, making decisions, generating output, and learning, such networks do not execute traditional computer programs. A physical neural network's capacities are determined by the type, specifications, and quantity of neurons that constitute the network.

## Third area: processes

This part of the ontology describes the key computational or cognitive processes carried out by the neuroprosthetic device that have implications for information security. Specific characteristics of this area are:

### Computational processes and computer control

While a neuroprosthetic device can potentially operate with full autonomy (or may be subject to control by the unconscious biological processes of its human host at a biochemical level, in the case of passive neuroprosthetic devices), such devices typically incorporate some means by which their users can exercise at least partial control over a device after its implantation. However, even a device that is ultimately controlled by a human user often still carries out some internal procedures for processing data in order to make

---

[55] See "FIPA Device Ontology Specification" (2002).

[56] See "FIPA Device Ontology Specification" (2002).

[57] See "FIPA Device Ontology Specification" (2002), and Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

decisions and generate actions.[58] The kinds of computational processes available to a neuroprosthetic device will depend on the kind of physical substrate upon which the processes are performed. The ontology includes specifications for a device's:

- **Level of autonomy**. As is the case for robotic systems, a neuroprosthetic device might function autonomously, semi-autonomously, or as a telepresence device under the full and direct control of its operator.[59] The level of autonomy is related to a neuroprosthetic device's:
  - **Capacity for control by its human host**,[60] as a device might be designed to respond to instructions delivered by its host via means such as oral verbal commands, instructions typed into a keypad or into the device's housing, or electrochemical signals from individual neurons or groups of neurons.[61]
  - **Capacity for control via teleoperation**, which may allow a neuroprosthetic device to be remotely controlled by external devices or by a user other than its human host.[62]
- **Computer programs** that can be run by a neuroprosthetic device utilizing a CPU-based system. The specifications for such a device should describe its:
  - **Operating system**,[63] which may be designed or installed by the device's manufacturer and include certain built-in diagnostic programs.
  - **Applications**[64] that can be stored and executed by the device to expand its functionality and which may be produced by its manufacturer, user, host, or third-party software developers.

---

[58] See Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[59] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[60] See "FIPA Device Ontology Specification" (2002) for information about user controls.

[61] See Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

[62] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[63] See "FIPA Device Ontology Specification" (2002) and Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

[64] See Clark & Fu, "Recent Results in Computer Security for Medical Devices" (2012).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

  - **Software update methods** that allow the device's operating system and applications to be modified after the device has been implanted in its human host.[65]

- **Neural computing** (if applicable). Here we use "neural computing" to describe the manner in which a neural network assimilates input and utilizes the information contained in its activation patterns to generate decisions and actions; this represents a means of computation different from the execution of traditional computer programs. A device that utilizes a physical neural network will thereby instantiate a neural computing process.[66] Some CPU-based systems may execute software that simulates a neural network,[67] however at their most fundamental level, such systems' computational processes are computer programs, not neural computing processes as defined here. At a minimum, the specifications of a neural computing process will describe: a) *the patterns of connection* between neurons; b) *the means by which connection weights are updated* (i.e., the learning mechanism); and 3) *the activation function* by which an individual neuron converts input to output.

## Input modalities and signals interpretable by the device

A neuroprosthetic device is typically capable of processing and interpreting certain kinds of signals received through its input mechanisms to extract or synthesize information (or perhaps even knowledge) that can potentially be compressed, stored, transmitted, transformed, and used to inform or control the device's operation.[68] A neuroprosthetic device may be able to recognize and extract meaning from input that arrives in the form of:

- **Machine communication protocols** such as TCP/IP, Bluetooth, 3G, and proprietary NFC formats.[69]
- **Environmental signals**. If a neuroprosthetic device possesses sufficiently advanced AI, it might be able to extract meaning directly from sensory input that it receives from the environment outside its host's

---

[65] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012), and McGee, "Bioelectronics and Implanted Devices" (2008).

[66] For an excellent discussion of the distinction between a physical neural network and the neural computational processes that may be occurring within it, see Mizraji et al., "Dynamic Searching in the Brain" (2009).

[67] See Merkel et al., "Central Neural Prostheses" (2007), and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[68] See Merkel et al., "Central Neural Prostheses" (2007).

[69] See "FIPA Device Ontology Specification" (2002); Li et al., "Advances and Challenges in Body Area Network" (2011); and Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009).

body. It may convert raw sensory data into modalities analogous to those that are accessible to human beings (such as identifiable sights, sounds, touches, tastes, smells, and proprioception that fall within the human range of perception).[70]

- **Natural human communication** which might be provided by the device's human host or user in the form of: a) *textual verbal input*[71] such as typed or emailed instructions that can be interpreted through an application of artificial intelligence; b) *oral verbal input*[72] such as spoken natural-language instructions that are identified through speech recognition software; and c) *nonverbal input*[73] such as gestures, eye gaze, or vocal intonation on the part of its human host or external user.
- **The host's biological processes**[74] which contain data such as those reflected in brain activity,[75] cardiac rhythms, and blood chemistry that can be interpreted by a neuroprosthetic device in a way that that recognizes particular patterns within the data that trigger some predetermined response. The patterns found in such data may or may not be under the conscious control of the device's host, depending on whether the data comprise: a) *the host's cognitive activity and patterns*,[76] which may include emotional states,[77] memories, volitions,[78] and sensory percepts; or b) *the host's motor activity and actions,* as even without direct access to the host's cognitive activity, a device might use techniques such as electromyography to detect and interpret electrical activity indicating voluntary contraction of a host's muscles.[79]

---

[70] See Merkel et al., "Central Neural Prostheses" (2007), and Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[71] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[72] See Rao & Nayak, *The InfoSec Handbook* (2014), and Merkel et al., "Central Neural Prostheses" (2007).

[73] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010), and Rao & Nayak, *The InfoSec Handbook* (2014).

[74] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[75] See Lebedev, "Brain-Machine Interfaces: An Overview" (2014).

[76] See McGee, "Bioelectronics and Implanted Devices" (2008).

[77] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[78] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[79] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement"

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Note that while a neuroprosthetic device might be able to receive and store many other kinds of input, only those forms of input whose modalities are interpretable by the device will typically have the potential to trigger purposeful and targeted responses by the device's computational processes.

## Output modalities and signals expressible by the device

In its capacity as an implantable computer, a neuroprosthetic device is typically capable of generating output in forms that can be interpreted by a human being or external device and which may carry specific meanings and may be used to influence or control the behavior of external entities in purposeful ways.[80] A device may be able to generate such output transmitted via:

- **Machine communication protocols** such as TCP/IP, Bluetooth, 3G, and proprietary NFC formats.[81]
- **Environmental signals**. If a neuroprosthetic device possesses sufficiently advanced computational processes, it might be able to directly encode messages in the form of physical output released into the environment external to its host's body or perhaps transmitted to its host through physical displays[82] or virtual reality equipment in the form of sensory modalities directly accessible to human beings (such as identifiable sights, sounds, touches, tastes, smells, and proprioception that fall within the human range of perception).
- **Natural human communication** which might take the form of: a) *textual verbal output*[83] provided to the device's host (e.g., either as messages appearing on a physical display screen on the device's visible housing or as messages overlaid in the host's field of vision, either through the use of an external virtual reality display or through the direct transmission of signals to the host's retinal ganglion cells, optic nerve, or interneurons in the brain) or to an external user (e.g., as messages displayed on an external accessory device or sent as ordinary emails); b) *oral verbal output*,[84] which might take the form of synthesized speech that is broadcast aloud through an external physical

---

(2012), and Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[80] See Merkel et al., "Central Neural Prostheses" (2007).

[81] See "FIPA Device Ontology Specification" (2002); Li et al., "Advances and Challenges in Body Area Network" (2011); and Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009).

[82] See "FIPA Device Ontology Specification" (2002).

[83] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

[84] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

speaker, that is "heard" by participants within some virtual reality environment, that is heard by the device's host through the direct transmission of signals to the host's cochlear nerve or to interneurons in the brain, or that might be generated by the host's own vocal cords, if the device is able to directly stimulate them; or c) *nonverbal output* such as gestures, eye gaze, or tone of voice, which could be displayed either by means of the device's control over its host's natural body, through the device's control of prosthetic components in the host's body, or through the device's manifestation as a digital avatar with a physical appearance within a virtual reality environment.

- **Host's biological processes** that can potentially be influenced or controlled by the device to produce particular phenomena such as brain activity, cardiac rhythms,[85] or changes in blood chemistry[86] that can be noticed and interpreted by the device's human host. Such patterns might be generated within: a) *the host's cognitive activity and patterns*, which may include the generation or alteration in the human host of emotional states, memories, volitions, and sensory percepts;[87] b) *the host's motor activity,*[88] through action of the device upon the host's efferent neurons or directly upon muscles; or c) *the control of other organs of the host,* by which the device influences or controls the functioning of other organs and systems within the host's body, either through direct electrochemical stimulation or through the manipulation of other systems within the host's body to trigger particular responses by organs.

Note that messages and information that a neuroprosthetic device transmits using these modalities may not have been generated by the device itself; e.g., they may have been stored in the device by its user in advance for later transmission, or they could be received live through some sensor and then immediately retransmitted by the device. It is also possible for such information to comprise an underlying stream of "real" sensory data from the external world that has been altered or augmented in some way, or it may be

---

[85] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[86] See McGee, "Bioelectronics and Implanted Devices" (2008).

[87] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); and Patil & Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices" (2008).

[88] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); McGee, "Bioelectronics and Implanted Devices" (2008); and Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

wholly fabricated within the neuroprosthetic device (or on an external device that transmits it to the neuroprosthetic device), to create a virtual reality environment to be experienced by the neuroprosthetic device's host. Such capacities could potentially be used in harmful (or at least manipulative) ways[89] if the device's functioning has been compromised by a virus or hacked by an unauthorized user.

## Fourth area: data, information, and knowledge received, generated, stored, and transmitted

The information security profile of an implantable neuroprosthetic device is shaped not only by the processes through which the device manipulates information or the physical locations in which the information is stored but also by the kinds of information involved.[90] Note that a neuroprosthetic device may be able to receive, generate, store, and transmit[91] types of information that the device itself cannot directly interpret or utilize (e.g., encrypted files that have been saved to the device by its user). This part of the ontology specifies the device's reception, storage, and transmission of:

### Data regarding the device's status and diagnostics

A neuroprosthetic device may handle information about its own internal status and functioning, which may be: a) *receivable by the device*, either from components internal to the device or from external monitors; b) *generated by the device*; c) *stored on the device* (e.g., in the form of logfiles); and d) *transmitted by the device* (e.g., to remote external components of the neuroprosthetic system or to medical personnel who are monitoring the device's status to ensure proper functioning).

### Environmental data

An implantable neuroprosthetic device may handle data about the environment exterior to its host's body similar to those gathered by human sensory organs.[92] Such information may be: a) *receivable by the device* through its own sensors or from afferent neurons in the host's body; b) *generated by the device*; c) *stored on the device* before or after undergoing processing; and d) *transmitted by the device* (e.g., to its human host as though it were sense data obtained directly by the host's own sensory organs, or to external systems or individuals who might use the data in teleoperation of the device).

---

[89] Regarding possibilities of neuroprosthetics being used to provide false data or information to their hosts or users, see McGee, "Bioelectronics and Implanted Devices" (2008), p. 221.

[90] See Rao & Nayak, *The InfoSec Handbook* (2014).

[91] See Li et al., "Advances and Challenges in Body Area Network" (2011).

[92] See McGee, "Bioelectronics and Implanted Devices" (2008).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

## Data regarding the host's physical status and biological processes

A neuroprosthetic device may handle highly sensitive information about the identity, location, health, and biological processes of its human host.[93] Such information may be: a) *receivable by the device* (e.g., through sensors directly monitoring the host's biological processes[94]); b) *generated by the device*; c) *stored on the device* after being gathered and processed by the device;[95] and d) *transmitted by the device* (e.g., through wireless communication to medical personnel who are remotely monitoring the host's medical condition and controlling the device to administer telemedicine services[96]).

## Data regarding the host's cognitive activity and patterns

In addition to information about more general biological processes, an implantable neuroprosthetic device with the appropriate form of neural connectivity could potentially receive, generate, store, and transmit – in at least limited fashion – information about the contents of its host's cognitive processes,[97] including emotional states, memories,[98] and volitions.[99] Such information might be: a) *receivable by the device* (e.g., through a BCI that can remotely detect activity in the host's brain or which interacts directly with interneurons in the brain through artificial synapses); b) *generated by the device* (e.g., through its analysis of other data); c) *stored on the device* for later processing and analysis, even if the device itself is incapable of performing such

---

[93] See Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010), and Kosta & Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants (2012).

[94] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[95] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[96] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012).

[97] See Gasson, "Human ICT Implants: From Restorative Application to Human Enhancement" (2012); Fairclough, "Physiological Computing: Interfacing with the Human Nervous System" (2010); Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009); and Widge et al., "Direct Neural Control of Anatomically Correct Robotic Hands" (2010).

[98] For the possibility of developing mnemoprosthetics, see Han et al., "Selective Erasure of a Fear Memory" (2009), and Ramirez et al., "Creating a False Memory in the Hippocampus" (2013).

[99] See McGee, "Bioelectronics and Implanted Devices" (2008).

analysis; and d) *transmitted by the device*[100] (e.g., to external medical systems for purposes of analyzing the user's neurological condition or to remote systems where the neural activity can be used to control prosthetic limbs or other robotic devices).

## Procedural knowledge

Procedural knowledge is the body of information needed to perform particular tasks; in the context of a neuroprosthetic device such knowledge might be: a) *receivable by the device* (e.g., in the form of downloadable packages that provide a device with instructions – perhaps including linguistic, social, and cultural information – on how to interact with its human host or user in particular situations); b) *generated by the device*; c) *stored on the device* (e.g., in the form of software[101] that guides the device's routine functioning and specifies how it should carry out particular actions in response to unique events or circumstances); and d) *transmitted by the device* (e.g., in the form of device drivers or other files sent to external devices to allow them to connect with the device and utilize its resources).

## Declarative knowledge

A neuroprosthetic device may handle descriptive or declarative knowledge in a format that is readily comprehensible to (and may have been prepared by) human beings.[102] This might include information contained in everyday correspondence like emails or text messages or the contents of documents downloaded from the Internet. Such information may be: a) *receivable by the device* (e.g., through electronic messages composed by the device's user, downloaded from websites through wireless Internet connections, or recorded in the form oral conversations that undergo speech-to-text processing); b) *generated by the device*; c) *stored on the device* (e.g., as ordinary text files); and d) *transmitted by the device* (e.g., in the form of messages or alerts sent to the device's human host or content downloaded from websites and available on demand for transmission to the host's sensory system for the host to experience).

---

[100] See Tarín et al., "Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring" (2009).

[101] See "FIPA Device Ontology Specification" (2002).

[102] See McGee, "Bioelectronics and Implanted Devices" (2008).

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

## Toward developing a comprehensive information security framework

In Figure 2 below we can see a sample representation of how the various parts of the ontology are instantiated and interrelate with one another in the case of a particular hypothetical implantable neuroprosthetic device.

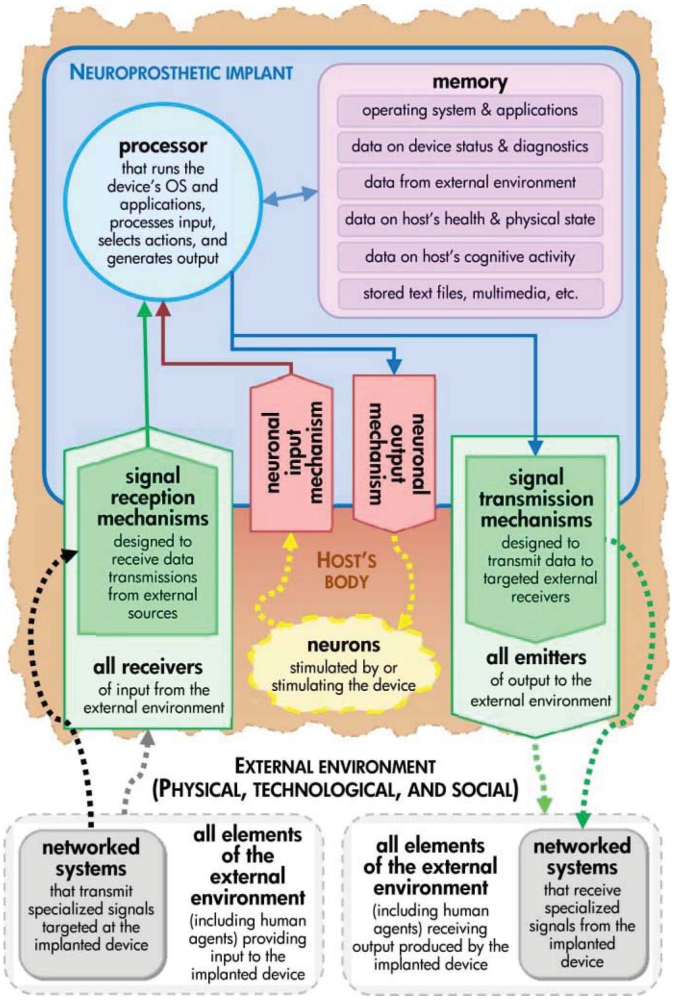

*Figure 2. One possible implementation of an implantable neuroprosthetic device, reflecting a unique profile of characteristics that can be captured and described by the device ontology for information security presented in this chapter.*

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

One can use this ontology to prepare an information security profile for a particular device by working through the ontology step-by-step and specifying the particular characteristics that the device (and its broader support system) possesses or demonstrates for each of the items. Once one possesses a completed ontology for a particular neuroprosthetic device – and thus understands its basic technical specifications and operational context – one can then apply the two-dimensional information security framework developed in the following chapter to understand the impacts that the device will have on its human host and the device's implications for the information security of its device-host system.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

# Bibliography

Abrams, Jerold J. "Pragmatism, Artificial Intelligence, and Posthuman Bioethics: Shusterman, Rorty, Foucault." *Human Studies* 27, no. 3 (September 1, 2004): 241-58. doi:10.1023/B:HUMA.0000042130.79208.c6.

Al-Hudhud, Ghada. "On Swarming Medical Nanorobots." *International Journal of Bio-Science & Bio-Technology* 4, no. 1 (March 2012): 75-90.

Ameen, Moshaddique Al, Jingwei Liu, and Kyungsup Kwak. "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications." *Journal of Medical Systems* 36, no. 1 (March 12, 2010): 93-101. doi:10.1007/s10916-010-9449-4.

Ankarali, Z.E., Q.H. Abbasi, A.F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan. "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security." In *2014 EAI 4th International Conference on Wireless Mobile Communication and Healthcare (Mobihealth)*, 246-49, 2014. doi:10.1109/MOBIHEALTH.2014.7015957.

Ansari, Sohail, K. Chaudhri, and K. Al Moutaery. "Vagus Nerve Stimulation: Indications and Limitations." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 281-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Armando, Alessandro, Gabriele Costa, Alessio Merlo, and Luca Verderame. "Formal Modeling and Automatic Enforcement of Bring Your Own Device Policies." *International Journal of Information Security*, (August 10, 2014): 1-18. doi:10.1007/s10207-014-0252-y.

Ayaz, Hasan, Patricia A. Shewokis, Scott Bunce, Maria Schultheis, and Banu Onaral. "Assessment of Cognitive Neural Correlates for a Functional Near Infrared-Based Brain Computer Interface System." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 699-708. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Baars, Bernard J. *In the Theater of Consciousness.* New York, NY: Oxford University Press, 1997.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Baddeley, Alan. "The episodic buffer: a new component of working memory?" *Trends in cognitive sciences* 4, no. 11 (2000): 417-423.

Baudrillard, Jean. *Simulacra and Simulation*. Ann Arbor: University of Michigan Press, 1994.

Berg, Bibi van den. "Pieces of Me: On Identity and Information and Communications Technology Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 159-73. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Bergamasco, S., M. Bon, and P. Inchingolo. "Medical data protection with a new generation of hardware authentication tokens." In *IFMBE Proceedings MEDICON 2001*, edited by R. Magjarevic, S. Tonkovic, V. Bilas, and I. Lackovic, 82-85. IFMBE, 2001.

Birbaumer, Niels, and Klaus Haagen. "Restoration of Movement and Thought from Neuroelectric and Metabolic Brain Activity: Brain-Computer Interfaces (BCIs)." In *Intelligent Computing Everywhere*, edited by Dr Alfons J. Schuster, 129-52. Springer London, 2007.

Birnbacher, Dieter. "Posthumanity, Transhumanism and Human Nature." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 95-106. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Borkar, Shekhar. "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation." *Micro, IEEE* 25, no. 6 (2005): 10-16.

Borton, D. A., Y.-K. Song, W. R. Patterson, C. W. Bull, S. Park, F. Laiwalla, J. P. Donoghue, and A. V. Nurmikko. "Implantable Wireless Cortical Recording Device for Primates." In *World Congress on Medical Physics and Biomedical Engineering, September 7-12, 2009, Munich, Germany*, edited by Olaf Dössel and Wolfgang C. Schlegel, 384-87. IFMBE Proceedings 25/9. Springer Berlin Heidelberg, 2009.

Bostrom, Nick. "Why I Want to Be a Posthuman When I Grow Up." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 107-36. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Bowman, Diana M., Mark N. Gasson, and Eleni Kosta. "The Societal Reality of That Which Was Once Science Fiction." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 175-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Braddon-Mitchell, David, and John Fitzpatrick. "Explanation and the Language of Thought." *Synthese* 83, no. 1 (April 1, 1990): 3-29. doi:10.1007/BF00413686.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Bradshaw, Jeffrey M., Paul Feltovich, Matthew Johnson, Maggie Breedy, Larry Bunch, Tom Eskridge, Hyuckchul Jung, James Lott, Andrzej Uszok, and Jurriaan van Diggelen. “From Tools to Teammates: Joint Activity in Human-Agent-Robot Teams.” In *Human Centered Design*, edited by Masaaki Kurosu, 935-44. Lecture Notes in Computer Science 5619. Springer Berlin Heidelberg, 2009.

Brey, Philip. “Ethical Aspects of Information Security and Privacy.” In *Security, Privacy, and Trust in Modern Data Management*, edited by Milan Petković and Willem Jonker, 21-36. Data-Centric Systems and Applications. Springer Berlin Heidelberg, 2007.

Brunner, Peter, and Gerwin Schalk. “Brain-Computer Interaction.” In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 719-23. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Buller, Tom. “Neurotechnology, Invasiveness and the Extended Mind.” *Neuroethics* 6, no. 3 (August 18, 2011): 593-605. doi:10.1007/s12152-011-9133-5.

Calverley, D.J. “Imagining a non-biological machine as a legal person.” *AI & SOCIETY* 22, no. 4 (2008): 523-37.

Campbell, Courtney S., James F. Keenan, David R. Loy, Kathleen Matthews, Terry Winograd, and Laurie Zoloth. “The Machine in the Body: Ethical and Religious Issues in the Bodily Incorporation of Mechanical Devices.” In *Altering Nature*, edited by B. Andrew Lustig, Baruch A. Brody, and Gerald P. McKenny, 199-257. Philosophy and Medicine 98. Springer Netherlands, 2008.

Cavallari, Maurizio. “Organisational Constraints on Information Systems Security.” In *Emerging Themes in Information Systems and Organization Studies*, edited by Andrea Carugati and Cecilia Rossignoli, 193-207. Physica-Verlag HD, 2011.

Cervera-Paz, Francisco Javier, and M. J. Manrique. “Auditory Brainstem Implants: Past, Present and Future Prospects.” In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 437-42. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Chadwick, Ruth. “Therapy, Enhancement and Improvement.” In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 25-37. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Chaudhry, Peggy E., Sohail S. Chaudhry, Ronald Reese, and Darryl S. Jones. “Enterprise Information Systems Security: A Conceptual Framework.” In *Re-Conceptualizing Enterprise Information Systems*, edited by Charles Møller

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

and Sohail Chaudhry, 118-28. Lecture Notes in Business Information Processing 105. Springer Berlin Heidelberg, 2012.

Cho, Kwantae, and Dong Hoon Lee. "Biometric Based Secure Communications without Pre-Deployed Key for Biosensor Implanted in Body Sensor Networks." In *Information Security Applications*, edited by Souhwan Jung and Moti Yung, 203-18. Lecture Notes in Computer Science 7115. Springer Berlin Heidelberg, 2012.

Church, George M., Yuan Gao, and Sriram Kosuri. "Next-generation digital information storage in DNA." *Science* 337, no. 6102 (2012): 1628.

Clark, Andy. "Systematicity, Structured Representations and Cognitive Architecture: A Reply to Fodor and Pylyshyn." In *Connectionism and the Philosophy of Mind*, edited by Terence Horgan and John Tienson, 198-218. Studies in Cognitive Systems 9. Springer Netherlands, 1991.

Clark, S.S., and K. Fu, "Recent Results in Computer Security for Medical Devices," in *Wireless Mobile Communication and Healthcare*, edited by K.S. Nikita, J.C. Lin, D.I. Fotiadis, and M.-T. Arredondo Waldmeyer, 111-18. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 83. Springer Berlin Heidelberg, 2012.

Claussen, Jens Christian, and Ulrich G. Hofmann. "Sleep, Neuroengineering and Dynamics." *Cognitive Neurodynamics* 6, no. 3 (May 27, 2012): 211-14. doi:10.1007/s11571-012-9204-2.

Clowes, Robert W. "The Cognitive Integration of E-Memory." *Review of Philosophy and Psychology* 4, no. 1 (January 26, 2013): 107-33. doi:10.1007/s13164-013-0130-y.

Coeckelbergh, M. "From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots." *Philosophy & Technology* 24, no. 3 (2011): 269-78.

Coles-Kemp, Lizzie, and Marianthi Theoharidou. "Insider Threat and Information Security Management." In *Insider Threats in Cyber Security*, edited by Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop, 45-71. Advances in Information Security 49. Springer US, 2010.

Cory, Jr., Gerald A. "Language, Brain, and Neuron." In *Toward Consilience*, 193-205. Springer US, 2000.

Cosgrove, G.R. (2004). "Session 6: Neuroscience, brain, and behavior V: Deep brain stimulation." Meeting of the President's Council on Bioethics. Washington, DC, June 24-25, 2004. https://bioethicsarchive.georgetown.edu/pcbe/transcripts/june04/session6.html. Accessed June 12, 2015.

Dardick, Glenn. "Cyber Forensics Assurance." In *Proceedings of the 8th Australian Digital Forensics Conference*, 57-64. Research Online, 2010.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Datteri, E. “Predicting the Long-Term Effects of Human-Robot Interaction: A Reflection on Responsibility in Medical Robotics.” *Science and Engineering Ethics* 19, no. 1 (2013): 139-60.

Delac, Kresimir, and Mislav Grgic. “A Survey of Biometric Recognition Methods.” In *Proceedings of the 46th International Symposium on Electronics in Marine, ELMAR 2004*, 184-93. IEEE, 2004.

Denning, Tamara, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno, and William H. Maisel. “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*, 917-26. ACM, 2010.

Denning, Tamara, Kevin Fu, and Tadayoshi Kohno. “Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security.” 3rd USENIX Workshop on Hot Topics in Security (HotSec 2008). San Jose, CA, July 29, 2008.

Denning, Tamara, Yoky Matsuoka, and Tadayoshi Kohno. “Neurosecurity: Security and Privacy for Neural Devices.” *Neurosurgical Focus* 27, no. 1 (2009): E7. doi:10.3171/2009.4.FOCUS0985.

Donchin, Emanuel, and Yael Arbel. “P300 Based Brain Computer Interfaces: A Progress Report.” In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 724-31. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Drongelen, Wim van, Hyong C. Lee, and Kurt E. Hecox. “Seizure Prediction in Epilepsy.” In *Neural Engineering*, edited by Bin He, 389-419. Bioelectric Engineering. Springer US, 2005.

Dudai, Yadin. “The Neurobiology of Consolidations, Or, How Stable Is the Engram?” *Annual Review of Psychology* 55 (2004): 51-86. doi:10.1146/annurev.psych.55.090902.142050.

Durand, Dominique M., Warren M. Grill, and Robert Kirsch. “Electrical Stimulation of the Neuromuscular System.” In *Neural Engineering*, edited by Bin He, 157-91. Bioelectric Engineering. Springer US, 2005.

Dvorsky, George. “What may be the world’s first cybernetic hate crime unfolds in French McDonald’s.” io9, July 17, 2012. http://io9.com/5926587/what-may-be-the-worlds-first-cybernetic-hate-crime-unfolds-in-french-mcdonalds. Accessed July 22, 2015.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Edgar, Andrew. “The Hermeneutic Challenge of Genetic Engineering: Habermas and the Transhumanists.” *Medicine, Health Care and Philosophy* 12, no. 2 (May 1, 2009): 157-67. doi:10.1007/s11019-009-9188-9.

Edlinger, Günter, Cristiano Rizzo, and Christoph Guger. “Brain Computer Interface.” In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 1003-17. Springer Berlin Heidelberg, 2011. http://link.springer.com/chapter/10.1007/978-3-540-74658-4_52.

Erler, Alexandre. “Does Memory Modification Threaten Our Authenticity?” *Neuroethics* 4, no. 3 (November 2011): 235-49. doi:10.1007/s12152-010-9090-4.

Fairclough, S.H. “Physiological Computing: Interfacing with the Human Nervous System.” In *Sensing Emotions*, edited by J. Westerink, M. Krans, and M. Ouwerkerk ,1-20. Philips Research Book Series 12. Springer Netherlands, 2010.

Fernandes, Diogo A. B., Liliana F. B. Soares, João V. Gomes, Mário M. Freire, and Pedro R. M. Inácio. “Security Issues in Cloud Environments: A Survey.” *International Journal of Information Security* 13, no. 2 (September 28, 2013): 113-70. doi:10.1007/s10207-013-0208-7.

Fernandez-Lopez, Helena, José A. Afonso, J. H. Correia, and Ricardo Simoes. “The Need for Standardized Tests to Evaluate the Reliability of Data Transport in Wireless Medical Systems.” In *Sensor Systems and Software*, edited by Francisco Martins, Luís Lopes, and Hervé Paulino, 137-45. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 102. Springer Berlin Heidelberg, 2012.

Ferrando, Francesca. “Posthumanism, Transhumanism, Antihumanism, Metahumanism, and New Materialisms: Differences and Relations.” *Existenz: An International Journal in Philosophy, Religion, Politics, and the Arts* 8, no. 2 (Fall 2013): 26-32.

“FIPA Device Ontology Specification.” Foundation for Intelligent Physical Agents (FIPA), May 10, 2002. http://www.fipa.org/assets/XC00091D.pdf. Accessed February 9, 2015.

Fleischmann, Kenneth R. “Sociotechnical Interaction and Cyborg–Cyborg Interaction: Transforming the Scale and Convergence of HCI.” *The Information Society* 25, no. 4 (2009): 227-35. doi:10.1080/01972240903028359.

Flemisch, F., M. Heesen, T. Hesse, J. Kelsch, A. Schieben, and J. Beller. “Towards a Dynamic Balance between Humans and Automation: Authority, Ability, Responsibility and Control in Shared and Cooperative Control Situations.” *Cognition, Technology & Work* 14, no. 1 (2012): 3-18. doi:10.1007/s10111-011-0191-6.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Fountas, Kostas N., and J. R. Smith. “A Novel Closed-Loop Stimulation System in the Control of Focal, Medically Refractory Epilepsy.” In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 357-62. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Fox, S. and L. Rainie. “The Web at 25 in the US: Part 1: How the Internet Has Woven Itself into American Life.” Pew Research Center’s Internet & American Life Project, February 27, 2014. http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life/. Accessed July 24, 2015.

Freudenthal, Eric, Ryan Spring, and Leonardo Estevez. “Practical techniques for limiting disclosure of RF-equipped medical devices.” In *Engineering in Medicine and Biology Workshop, 2007 IEEE Dallas*, 82-85. IEEE, 2007.

Friedenberg, Jay. *Artificial Psychology: The Quest for What It Means to Be Human*, Philadelphia: Psychology Press, 2011.

Gärtner, Armin. “Communicating Medical Systems and Networks.” In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 1085-93. Springer Berlin Heidelberg, 2011.

Gasson, M.N., Kosta, E., and Bowman, D.M. “Human ICT Implants: From Invasive to Pervasive.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 1-8. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Gasson, M.N. “Human ICT Implants: From Restorative Application to Human Enhancement.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 11-28. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Gasson, M.N. “ICT implants.” In *The Future of Identity in the Information Society*, edited by S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci, 287-95. Springer US, 2008.

Gerhardt, Greg A., and Patrick A. Tresco. “Sensor Technology.” In *Brain-Computer Interfaces*, 7-29. Springer Netherlands, 2008.

Gladden, Matthew E. “Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values.” Ethics in Economic Life. Uniwersytet Łódzki, Łódź, May 8, 2015.

Gladden, Matthew E. “Cybershells, Shapeshifting, and Neuroprosthetics: Video Games as Tools for Posthuman ‘Body Schema (Re)Engineering’.” Ogólnopolska Konferencja Naukowa Dyskursy Gier Wideo. Facta Ficta, AGH, Kraków, June 6, 2015.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Gladden, Matthew E. "A Fractal Measure for Comparing the Work Effort of Human and Artificial Agents Performing Management Functions." In *Position Papers of the 2014 Federated Conference on Computer Science and Information Systems*, edited by Maria Ganzha, Leszek Maciaszek, Marcin Paprzycki, 219-26. Annals of Computer Science and Information Systems 3. Polskie Towarzystwo Informatyczne, 2014.

Gladden, Matthew E. "Neural Implants as Gateways to Socioeconomic Interaction and Posthuman Informational Ecosystems." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.

Gladden, Matthew E. "The Social Robot as 'Charismatic Leader': A Phenomenology of Human Submission to Nonhuman Power." In *Sociable Robots and the Future of Social Relations: Proceedings of Robo-Philosophy 2014*, edited by Johanna Seibt, Raul Hakli, and Marco Nørskov, 329-39. Frontiers in Artificial Intelligence and Applications 273. IOS Press, 2014.

Gladden, Matthew E. "Tachikomatic Domains: Utopian Cyberspace as a 'Contingent Heaven' for Humans, Robots, and Hybrid Intelligences." His Master's Voice: Utopias and Dystopias in Audiovisual Culture. Facta Ficta, Jagiellonian University, Kraków, March 24, 2015.

Gladden, Matthew E. "'Upgrading' the Human Entity: Cyberization as a Path to Posthuman Utopia or Digital Annihilation?" Arkana Fantastyki lecture cycle. Centrum Informacji Naukowej i Biblioteka Akademicka (CINiBA), Katowice, May 27, 2015.

Gordijn, Bert. "Converging NBIC Technologies for Improving Human Performance." In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 225-35. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Greenberg, Andy. "Cyborg Discrimination? Scientist Says McDonald's Staff Tried To Pull Off His Google-Glass-Like Eyepiece, Then Threw Him Out." Forbes, July 17, 2012. http://www.forbes.com/sites/andygreenberg/2012/07/17/cyborg-discrimination-scientist-says-mcdonalds-staff-tried-to-pull-off-his-google-glass-like-eyepiece-then-threw-him-out/. Accessed July 22, 2015.

Grodzinsky, F.S., K.W. Miller, and M.J. Wolf. "Developing Artificial Agents Worthy of Trust: 'Would You Buy a Used Car from This Artificial Agent?'" *Ethics and Information Technology* 13, no. 1 (2011): 17-27.

Grottke, M., H. Sun, R. M. Fricks, and K. S. Trivedi. "Ten fallacies of availability and reliability analysis." In *Service Availability*, 187-206. Lecture Notes in Computer Science 5017. Springer Berlin Heidelberg, 2008. http://dx.doi.org/10.1007/978-3-540-68129-8_15.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Gunkel, David, and Debra Hawhee. "Virtual Alterity and the Reformatting of Ethics." *Journal of Mass Media Ethics* 18, no. 3-4 (2003): 173-93. doi:10.1080/08900523.2003.9679663.

Gunther, N. J. "Time—the zeroth performance metric." In *Analyzing Computer System Performance with Perl::PDQ*, 3-46. Berlin: Springer, 2005. http://dx.doi.org/10.1007/978-3-540-26860-4_1.

Halperin, Daniel, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses." In *IEEE Symposium on Security and Privacy, 2008. SP 2008*, 129-142. IEEE, 2008.

Halperin, Daniel, Tadayoshi Kohno, Thomas S. Heydt-Benjamin, Kevin Fu, and William H. Maisel. "Security and privacy for implantable medical devices." *Pervasive Computing, IEEE* 7, no. 1 (2008): 30-39.

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

Hansen, Jeremy A., and Nicole M. Hansen. "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*, 13-20. ACM, 2010.

Hanson, R. (1994). "If uploads come first: The crack of a future dawn." *Extropy* 6, no. 2 (1994), 10-15.

Harrison, Ian. "IEC80001 and Future Ramifications for Health Systems Not Currently Classed as Medical Devices." In *Making Systems Safer*, edited by Chris Dale and Tom Anderson, 149-71. Springer London, 2010.

Hatfield, B., A. Haufler, and J. Contreras-Vidal. "Brain Processes and Neurofeedback for Performance Enhancement of Precision Motor Behavior." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen, 810-17. Lecture Notes in Computer Science 5638. Springer Berlin Heidelberg, 2009.

Hei, Xiali, and Xiaojiang Du. "Biometric-based two-level secure access control for implantable medical devices during emergencies." In *INFOCOM, 2011 Proceedings IEEE*, 346-350. IEEE, 2011.

Heersmink, Richard. "Embodied Tools, Cognitive Tools and Brain-Computer Interfaces." *Neuroethics* 6, no. 1 (September 1, 2011): 207-19. doi:10.1007/s12152-011-9136-2.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Hellström, T. "On the Moral Responsibility of Military Robots," *Ethics and Information Technology* 15, no. 2 (2013): 99-107.

Hern, Alex. "Hacker fakes German minister's fingerprints using photos of her hands." The Guardian, December 30, 2014. http://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands. Accessed July 24, 2015.

Hildebrandt, Mireille, and Bernhard Anrig. "Ethical Implications of ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 135-58. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Hoffmann, Klaus-Peter, and Silvestro Micera. "Introduction to Neuroprosthetics." In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 785-800. Springer Berlin Heidelberg, 2011.

Humphreys, L., J. M. Ferrández, and E. Fernández. "Long Term Modulation and Control of Neuronal Firing in Excitable Tissue Using Optogenetics." In *Foundations on Natural and Artificial Computation*, edited by José Manuel Ferrández, José Ramón Álvarez Sánchez, Félix de la Paz, and F. Javier Toledo, 266-73. Lecture Notes in Computer Science 6686. Springer Berlin Heidelberg, 2011.

Illes, Judy. Neuroethics: Defining the Issues in Theory, Practice, and Policy. Oxford University Press, 2006.

Josselyn, Sheena A. "Continuing the Search for the Engram: Examining the Mechanism of Fear Memories." *Journal of Psychiatry & Neuroscience : JPN* 35, no. 4 (July 2010): 221-28. doi:10.1503/jpn.100015.

Katz, Gregory. "The Hypothesis of a Genetic Protolanguage: An Epistemological Investigation." *Biosemiotics* 1, no. 1 (February 8, 2008): 57-73. doi:10.1007/s12304-008-9005-5.

Kirkpatrick, K. "Legal Issues with Robots." *Communications of the ACM* 56, no. 11 (2013): 17-19.

KleinOsowski, A., Ethan H. Cannon, Phil Oldiges, and Larry Wissel. "Circuit design and modeling for soft errors." *IBM Journal of Research and Development* 52, no. 3 (2008): 255-63.

Kłoda-Staniecko, Bartosz. "Ja, Cyborg. Trzy porządki, jeden byt. Podmiot jako fuzja biologii, kultury i technologii" ("I, Cyborg. Three Orders, One Being. Subject as a Fusion of Nature, Culture and Technology"). In *Człowiek w relacji do zwierząt, roślin i maszyn w kulturze: Tom I: Aspekt posthumanistyczny i transhumanistyczny*, edited by Justyny Tymienieckiej-Suchanek. Uniwersytet Śląski, 2015.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Koch, K. P. "Neural Prostheses and Biomedical Microsystems in Neurological Rehabilitation." In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 427-34. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Koebler, Jason. "FCC Cracks Down on Cell Phone 'Jammers': The FCC says illegal devices that block cell phone signals could pose security risk." U.S. News & World Report, October 17, 2012. http://www.usnews.com/news/articles/2012/10/17/fcc-cracks-down-on-cell-phone-jammers. Accessed July 22, 2015.

Koene, Randal A. "Embracing Competitive Balance: The Case for Substrate-Independent Minds and Whole Brain Emulation." In *Singularity Hypotheses*, edited by Amnon H. Eden, James H. Moor, Johnny H. Søraker, and Eric Steinhart, 241-67. The Frontiers Collection. Springer Berlin Heidelberg, 2012.

Kolkowska, Ella, and Gurpreet Dhillon. "Organizational Power and Information Security Rule Compliance." In *Future Challenges in Security and Privacy for Academia and Industry*, edited by Jan Camenisch, Simone Fischer-Hübner, Yuko Murayama, Armand Portmann, and Carlos Rieder, 185-96. IFIP Advances in Information and Communication Technology 354. Springer Berlin Heidelberg, 2011.

Koops, B.-J., and R. Leenes (2012). "Cheating with Implants: Implications of the Hidden Information Advantage of Bionic Ears and Eyes." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 113-34. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Kosta, E., and D.M. Bowman, "Implanting Implications: Data Protection Challenges Arising from the Use of Human ICT Implants." In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 97-112. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

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

Kowalewska, Agata. "Symbionts and Parasites – Digital Ecosystems." Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.

Kraemer, Felicitas. "Me, Myself and My Brain Implant: Deep Brain Stimulation Raises Questions of Personal Authenticity and Alienation." *Neuroethics* 6, no. 3 (May 12, 2011): 483-97. doi:10.1007/s12152-011-9115-7.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Kuflik, A. “Computers in Control: Rational Transfer of Authority or Irresponsible Abdication of Autonomy?” *Ethics and Information Technology* 1, no. 3 (1999): 173-84.

Lebedev, M., “Brain-Machine Interfaces: An Overview,” *Translational Neuroscience* 5, no. 1 (March 28, 2014): 99-110.

Leder, Felix, Tillmann Werner, and Peter Martini. “Proactive Botnet Countermeasures: An Offensive Approach.” In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 211-25. Cryptology and Information Security Series. IOS Press, 2009. doi:10.3233/978-1-60750-060-5-211.

Lee, Giljae, Andréa Matsunaga, Salvador Dura-Bernal, Wenjie Zhang, William W. Lytton, Joseph T. Francis, and José AB Fortes. “Towards Real-Time Communication between in Vivo Neurophysiological Data Sources and Simulator-Based Brain Biomimetic Models.” *Journal of Computational Surgery* 3, no. 1 (November 11, 2014): 1-23. doi:10.1186/s40244-014-0012-3.

Li, S., F. Hu, and G. Li, “Advances and Challenges in Body Area Network.” In *Applied Informatics and Communication*, edited by J. Zhan, 58-65. Communications in Computer and Information Science 22. Springer Berlin Heidelberg, 2011.

Linsenmeier, Robert A. “Retinal Bioengineering.” In *Neural Engineering*, edited by Bin He, 421-84. Bioelectric Engineering. Springer US, 2005.

Lloyd, David. “Biological Time Is Fractal: Early Events Reverberate over a Life Time.” *Journal of Biosciences* 33, no. 1 (March 1, 2008): 9–19. doi:10.1007/s12038-008-0017-8.

Longuet-Higgins, H.C. “Holographic Model of Temporal Recall.” *Nature* 217, no. 5123 (1968): 104. doi:10.1038/217104a0.

Lorence, Daniel, Anusha Sivaramakrishnan, and Michael Richards. “Transaction-Neutral Implanted Data Collection Interface as EMR Driver: A Model for Emerging Distributed Medical Technologies.” *Journal of Medical Systems* 34, no. 4 (March 20, 2009): 609-17. doi:10.1007/s10916-009-9274-9.

Lucivero, Federica, and Guglielmo Tamburrini. “Ethical Monitoring of Brain-Machine Interfaces.” *AI & SOCIETY* 22, no. 3 (August 3, 2007): 449-60. doi:10.1007/s00146-007-0146-x.

Ma, Ting, Ying-Ying Gu, and Yuan-Ting Zhang. “Circuit Models for Neural Information Processing.” In *Neural Engineering*, edited by Bin He, 333-65. Bioelectric Engineering. Springer US, 2005.

MacVittie, Kevin, Jan Halámek, Lenka Halámková, Mark Southcott, William D. Jemison, Robert Lobel, and Evgeny Katz. “From ‘cyborg’ lobsters to a pacemaker powered by implantable biofuel cells.” *Energy & Environmental Science* 6, no. 1 (2013): 81-86.

Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.

Maj, Krzysztof. “Rational Technotopia vs. Corporational Dystopia in ‘Deus Ex: Human Revolution’ Gameworld.” His Master's Voice: Utopias and Dystopias in Audiovisual Culture. Facta Ficta, Jagiellonian University, Kraków, March 24, 2015.

Mak, Stephen. “Ethical Values for E-Society: Information, Security and Privacy.” In *Ethics and Policy of Biometrics*, edited by Ajay Kumar and David Zhang, 96-101. Lecture Notes in Computer Science 6005. Springer Berlin Heidelberg, 2010.

Masani, Kei, and Milos R. Popovic. “Functional Electrical Stimulation in Rehabilitation and Neurorehabilitation.” In *Springer Handbook of Medical Technology*, edited by Rüdiger Kramme, Klaus-Peter Hoffmann, and Robert S. Pozos, 877-96. Springer Berlin Heidelberg, 2011.

McCormick, Michael. “Data Theft: A Prototypical Insider Threat.” In *Insider Attack and Cyber Security*, edited by Salvatore J. Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Shlomo Hershkop, Sean W. Smith, and Sara Sinclair, 53-68. Advances in Information Security 39. Springer US, 2008.

McCullagh, P., G. Lightbody, J. Zygierewicz, and W.G. Kernohan, “Ethical Challenges Associated with the Development and Deployment of Brain Computer Interface Technology.” *Neuroethics* 7, no. 2 (July 28, 2013): 109-22.

McGee, E.M., “Bioelectronics and Implanted Devices.” In *Medical Enhancement and Posthumanity*, edited by B. Gordijn and R. Chadwick, 207-24. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

McGrath, Michael J., and Cliodhna Ní Scanaill. “Regulations and Standards: Considerations for Sensor Technologies.” In *Sensor Technologies*, 115-35. Apress, 2013.

Meloy, Stuart. “Neurally Augmented Sexual Function.” In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 359-63. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Merkel, R., G. Boer, J. Fegert, T. Galert, D. Hartmann, B. Nuttin, and S. Rosahl, “Central Neural Prostheses.” In *Intervening in the Brain: Changing Psyche and Society*, 117-60. Ethics of Science and Technology Assessment 29. Springer Berlin Heidelberg, 2007.

Miah, Andy. “A Critical History of Posthumanism.” In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 71-94. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics," an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics, ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Miller, Kai J., and Jeffrey G. Ojemann. "A Simple, Spectral-Change Based, Electrocorticographic Brain–Computer Interface." In *Brain-Computer Interfaces*, edited by Bernhard Graimann, Gert Pfurtscheller, and Brendan Allison, 241-58. The Frontiers Collection. Springer Berlin Heidelberg, 2009.

Mitcheson, Paul D. "Energy harvesting for human wearable and implantable bio-sensors." In *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE,* 3432-3436. IEEE, 2010.

Mizraji, Eduardo, Andrés Pomi, and Juan C. Valle-Lisboa. "Dynamic Searching in the Brain." *Cognitive Neurodynamics* 3, no. 4 (June 3, 2009): 401-14. doi:10.1007/s11571-009-9084-2.

Moravec, Hans. *Mind Children: The Future of Robot and Human Intelligence*. Cambridge: Harvard University Press, 1990.

Moxon, Karen A. "Neurorobotics." In *Neural Engineering*, edited by Bin He, 123-55. Bioelectric Engineering. Springer US, 2005.

Negoescu, R. "Conscience and Consciousness in Biomedical Engineering Science and Practice." In *International Conference on Advancements of Medicine and Health Care through Technology*, edited by Simona Vlad, Radu V. Ciupa, and Anca I. Nicu, 209-14. IFMBE Proceedings 26. Springer Berlin Heidelberg, 2009.

Neuper, Christa, and Gert Pfurtscheller. "Neurofeedback Training for BCI Control." In *Brain-Computer Interfaces*, edited by Bernhard Graimann, Gert Pfurtscheller, and Brendan Allison, 65-78. The Frontiers Collection. Springer Berlin Heidelberg, 2009.

*NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security*. Edited by Gary Stoneburner. Gaithersburg, Maryland: National Institute of Standards & Technology, 2001.

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

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

*NIST Special Publication 800-70, Revision 2: National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*. Edited by Stephen D. Quinn, Murugiah P. Souppaya, Melanie Cook, and Karen A. Scarfone. Gaithersburg, Maryland: National Institute of Standards & Technology, 2011.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

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

Overman, Stephenie. "Jamming Employee Phones Illegal." Society for Human Resource Management, May 9, 2014. http://www.shrm.org/hrdisciplines/technology/articles/pages/cell-phone-jamming.aspx. Accessed July 22, 2015.

Pająk, Robert. Email correspondence with the author, May 3, 2015.

Panoulas, Konstantinos J., Leontios J. Hadjileontiadis, and Stavros M. Panas. "Brain-Computer Interface (BCI): Types, Processing Perspectives and Applications." In *Multimedia Services in Intelligent Environments*, edited by George A. Tsihrintzis and Lakhmi C. Jain, 299-321. Smart Innovation, Systems and Technologies 3. Springer Berlin Heidelberg, 2010.

Park, M.C., M.A. Goldman, T.W. Belknap, and G.M. Friehs, "The Future of Neural Interface Technology." In *Textbook of Stereotactic and Functional Neurosurgery*, edited by A.M. Lozano, P.L. Gildenberg, and R.R. Tasker, 3185-3200. Heidelberg/Berlin: Springer, 2009.

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

Parker, Donn B. "Toward a New Framework for Information Security." In *The Computer Security Handbook*, 4th Ed., edited by Seymour Bosworth and M. E. Kabay. John Wiley & Sons, 2002.

Passeraub, Ph A., and N. V. Thakor. "Interfacing Neural Tissue with Microsystems." In *Neural Engineering*, edited by Bin He, 49-83. Bioelectric Engineering. Springer US, 2005.

Patil, P.G., and D.A. Turner, "The Development of Brain-Machine Interface Neuroprosthetic Devices." In *Neurotherapeutics* 5, no. 1 (January 1, 2008): 137-46.

Pearce, David, "The Biointelligence Explosion." In *Singularity Hypotheses*, edited by A.H. Eden, J.H. Moor, J.H. Søraker, and E. Steinhart, 199-238. The Frontiers Collection. Berlin/Heidelberg: Springer, 2012.

Polikov, Vadim S., Patrick A. Tresco, and William M. Reichert. "Response of brain tissue to chronically implanted neural electrodes." *Journal of Neuroscience Methods* 148, no. 1 (2005): 1-18.

Prestes, E., J.L. Carbonera, S. Rama Fiorini, V.A.M. Jorge, M. Abel, R. Madhavan, A. Locoro, et al., "Towards a Core Ontology for Robotics and Automation." *Robotics and Autonomous Systems*, Ubiquitous Robotics 61, no. 11 (November 2013): 1193-1204.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Pribram, K. H. "Prolegomenon for a Holonomic Brain Theory." In *Synergetics of Cognition*, edited by Hermann Haken and Michael Stadler, 150-84. Springer Series in Synergetics 45. Springer Berlin Heidelberg, 1990.

Pribram, K.H., and S.D. Meade. "Conscious Awareness: Processing in the Synaptodendritic Web - The Correlation of Neuron Density with Brain Size." *New Ideas in Psychology* 17, no. 3 (December 1, 1999): 205–14. doi:10.1016/S0732-118X(99)00024-0.

Principe, José C., and Dennis J. McFarland. "BMI/BCI Modeling and Signal Processing." In *Brain-Computer Interfaces*, 47-64. Springer Netherlands, 2008.

Proudfoot, Diane. "Software Immortals: Science or Faith?" In *Singularity Hypotheses*, edited by Amnon H. Eden, James H. Moor, Johnny H. Søraker, and Eric Steinhart, 367-92. The Frontiers Collection. Springer Berlin Heidelberg, 2012.

Qureshi, Mohmad Kashif. "Liveness detection of biometric traits." *International Journal of Information Technology and Knowledge Management* 4 (2011): 293-95.

Rahimi, Ali, Ben Recht, Jason Taylor, and Noah Vawter. "On the effectiveness of aluminium foil helmets: An empirical study." MIT, February 17, 2005. http://web.archive.org/web/20100708230258/http://people.csail.mit.edu/rahimi/helmet/. Accessed July 26, 2015.

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

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

Rao, Umesh Hodeghatta, and Umesha Nayak. *The InfoSec Handbook*. New York: Apress, 2014.

Rasmussen, Kasper Bonne, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. "Proximity-based access control for implantable medical devices." In *Proceedings of the 16th ACM conference on Computer and communications security*, 410-19. ACM, 2009.

Reynolds, Dwight W., Christina M. Murray, and Robin E. Germany. "Device Therapy for Remote Patient Management." In *Electrical Diseases of the Heart*, edited by Ihor Gussak, Charles Antzelevitch, Arthur A. M. Wilde, Paul A. Friedman, Michael J. Ackerman, and Win-Kuang Shen, 809-25. Springer London, 2008.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Robinett, W. “The consequences of fully understanding the brain.” In Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science, edited by M.C. Roco and W.S. Bainbridge, 166-70. National Science Foundation, 2002.

Roosendaal, Arnold. “Carrying Implants and Carrying Risks; Human ICT Implants and Liability.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 69-79. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Roosendaal, Arnold. “Implants and Human Rights, in Particular Bodily Integrity.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 81-96. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rossebeø, J. E. Y., M. S. Lund, K. E. Husa, and A. Refsdal, “A conceptual model for service availability.” In *Quality of Protection*, 107-18. Advances in Information Security 23. Springer US, 2006.

Rotter, Pawel, Barbara Daskala, and Ramon Compañó. “Passive Human ICT Implants: Risks and Possible Solutions.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 55-62. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rotter, Pawel, Barbara Daskala, Ramon Compañó, Bernhard Anrig, and Claude Fuhrer. “Potential Application Areas for RFID Implants.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 29-39. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rotter, Pawel, and Mark N. Gasson. “Implantable Medical Devices: Privacy and Security Concerns.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 63-66. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Rubin, Charles T. “What Is the Good of Transhumanism?” In *Medical Enhancement and Posthumanity*, edited by Bert Gordijn and Ruth Chadwick, 137-56. The International Library of Ethics, Law and Technology 2. Springer Netherlands, 2008.

Rutten, W. L. C., T. G. Ruardij, E. Marani, and B. H. Roelofsen. “Neural Networks on Chemically Patterned Electrode Arrays: Towards a Cultured Probe.” In *Operative Neuromodulation*, edited by Damianos E. Sakas and

Brian A. Simpson, 547-54. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Sakas, Damianos E., I. G. Panourias, and B. A. Simpson. “An Introduction to Neural Networks Surgery, a Field of Neuromodulation Which Is Based on Advances in Neural Networks Science and Digitised Brain Imaging.” In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 3-13. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Sasse, Martina Angela, Sacha Brostoff, and Dirk Weirich. “Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security.” *BT technology journal* 19, no. 3 (2001): 122-131.

Sayrafian-Pour, K., W.-B. Yang, J. Hagedorn, J. Terrill, K. Yekeh Yazdandoost, and K. Hamaguchi. “Channel Models for Medical Implant Communication.” *International Journal of Wireless Information Networks* 17, no. 3-4 (December 9, 2010): 105-12.

Schechter, Stuart. “Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices.” Microsoft Research, August 10, 2010. http://research.microsoft.com:8082/apps/pubs/default.aspx?id=135291. Accessed July 26, 2015.

Schermer, Maartje. “The Mind and the Machine. On the Conceptual and Moral Implications of Brain-Machine Interaction.” *NanoEthics* 3, no. 3 (December 1, 2009): 217-30. doi:10.1007/s11569-009-0076-9.

Shih, J. “Project time in Silicon Valley.” *Qualitative Sociology* 27, no. 2 (June 1, 2004): 223-45.

Shoniregun, Charles A., Kudakwashe Dube, and Fredrick Mtenzi. “Introduction to E-Healthcare Information Security.” In *Electronic Healthcare Information Security*, 1-27. Advances in Information Security 53. Springer US, 2010.

Smolensky, Paul. “The Constituent Structure of Connectionist Mental States: A Reply to Fodor and Pylyshyn.” In *Connectionism and the Philosophy of Mind*, edited by Terence Horgan and John Tienson, 281-308. Studies in Cognitive Systems 9. Springer Netherlands, 1991.

Soussou, Walid V., and Theodore W. Berger. “Cognitive and Emotional Neuroprostheses.” In *Brain-Computer Interfaces*, 109-23. Springer Netherlands, 2008.

Spohrer, Jim, “NBICS (Nano-Bio-Info-Cogno-Socio) Convergence to Improve Human Performance: Opportunities and Challenges.” In Converging Technologies for Improving Human Performance: Nanotechnology, Biotechnology, Information Technology and Cognitive Science, edited by M.C. Roco and W.S. Bainbridge, 101-17. Arlington, Virginia: National Science Foundation, 2002.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Srinivasan, G. R. “Modeling the cosmic-ray-induced soft-error rate in integrated circuits: an overview.” *IBM Journal of Research and Development* 40, no. 1 (1996): 77-89.

Stahl, B. C. “Responsible Computers? A Case for Ascribing Quasi-Responsibility to Computers Independent of Personhood or Agency.” *Ethics and Information Technology* 8, no. 4 (2006): 205-13.

Stieglitz, Thomas. “Restoration of Neurological Functions by Neuroprosthetic Technologies: Future Prospects and Trends towards Micro-, Nano-, and Biohybrid Systems.” In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 435-42. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Szczepocka, Magdalena. “Konflikt sprzecznych utopii jako główny problem gry fabularnej ‘Mag: Wstąpienie’.” Głos Pana: Utopie i dystopie w kulturze audiowizualnej. Facta Ficta, Jagiellonian University, Kraków, March 27, 2015.

Tadeusiewicz, Ryszard, Pawel Rotter, and Mark N. Gasson. “Restoring Function: Application Exemplars of Medical ICT Implants.” In *Human ICT Implants: Technical, Legal and Ethical Considerations*, edited by Mark N. Gasson, Eleni Kosta, and Diana M. Bowman, 41-51. Information Technology and Law Series 23. T. M. C. Asser Press, 2012.

Taira, Takaomi, and T. Hori. “Diaphragm Pacing with a Spinal Cord Stimulator: Current State and Future Directions.” In *Operative Neuromodulation*, edited by Damianos E. Sakas, Brian A. Simpson, and Elliot S. Krames, 289-92. Acta Neurochirurgica Supplements 97/1. Springer Vienna, 2007.

Tamburrini, Guglielmo. “Brain to Computer Communication: Ethical Perspectives on Interaction Models.” *Neuroethics* 2, no. 3 (March 11, 2009): 137-49. doi:10.1007/s12152-009-9040-1.

Tarín, C., L. Traver, P. Martí, and N. Cardona. “Wireless Communication Systems from the Perspective of Implantable Sensor Networks for Neural Signal Monitoring.” In *Wireless Technology*, edited by S. Powell and J.P. Shim, 177-201. Lecture Notes in Electrical Engineering 44. Springer US, 2009.

Taylor, N. R., and J. G. Taylor. “The Neural Networks for Language in the Brain: Creating LAD.” In *Computational Models for Neuroscience*, edited by Robert Hecht-Nielsen and Thomas McKenna, 245-65. Springer London, 2003.

Taylor, Dawn M. “Functional Electrical Stimulation and Rehabilitation Applications of BCIs.” In *Brain-Computer Interfaces*, 81-94. Springer Netherlands, 2008.

Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"
an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,
ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.

Thanos, Solon, P. Heiduschka, and T. Stupp. "Implantable Visual Prostheses." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 465-72. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

Thonnard, Olivier, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, and Martin Lee. "Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat." In *Research in Attacks, Intrusions, and Defenses*, edited by Davide Balzarotti, Salvatore J. Stolfo, and Marco Cova, 64-85. Lecture Notes in Computer Science 7462. Springer Berlin Heidelberg, 2012.

Thorpe, Julie, Paul C. van Oorschot, and Anil Somayaji. "Pass-thoughts: authenticating with our minds." In *Proceedings of the 2005 Workshop on New Security Paradigms*, 45-56. ACM, 2005.

Troyk, Philip R., and Stuart F. Cogan. "Sensory Neural Prostheses." In *Neural Engineering*, edited by Bin He, 1-48. Bioelectric Engineering. Springer US, 2005.

Ullah, Sana, Henry Higgin, M. Arif Siddiqui, and Kyung Sup Kwak. "A Study of Implanted and Wearable Body Sensor Networks." In *Agent and Multi-Agent Systems: Technologies and Applications*, edited by Ngoc Thanh Nguyen, Geun Sik Jo, Robert J. Howlett, and Lakhmi C. Jain, 464-73. Lecture Notes in Computer Science 4953. Springer Berlin Heidelberg, 2008.

U.S. Code, Title 44 (Public Printing and Documents), Subchapter III (Information Security), Section 3542 (Definitions), cited in *NIST Special Publication 800-37, Revision 1*.

Vildjiounaite, Elena, Satu-Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, and Heikki Ailisto. "Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices." In *Pervasive Computing*, edited by Kenneth P. Fishkin, Bernt Schiele, Paddy Nixon, and Aaron Quigley, 187-201. Lecture Notes in Computer Science 3968. Springer Berlin Heidelberg, 2006.

Viola, M. V., and Aristides A. Patrinos. "A Neuroprosthesis for Restoring Sight." In *Operative Neuromodulation*, edited by Damianos E. Sakas and Brian A. Simpson, 481-86. Acta Neurochirurgica Supplements 97/2. Springer Vienna, 2007.

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

Warwick, K., and M. Gasson, "Implantable Computing." In *Digital Human Modeling*, edited by Y. Cai, 1-16. Lecture Notes in Computer Science 4650. Berlin/Heidelberg: Springer, 2008.

Weber, R. H., and Weber, R. "General Approaches for a Legal Framework." In *Internet of Things*, 23-40. Springer Berlin/Heidelberg, 2010.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Weiland, James D., Wentai Liu, and Mark S. Humayun. “Retinal Prosthesis.” *Annual Review of Biomedical Engineering* 7, no. 1 (2005): 361-401. doi:10.1146/annurev.bioeng.7.060804.100435.

Weinberger, Sharon. “Mind Games.” The Washington Post, January 14, 2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399_pf.html. Accessed July 26, 2015.

Werkhoven, Peter. “Experience Machines: Capturing and Retrieving Personal Content.” In *E-Content*, edited by Peter A. Bruck, Zeger Karssen, Andrea Buchholz, and Ansgar Zerfass, 183-202. Springer Berlin Heidelberg, 2005.

Widge, A.S., C.T. Moritz, and Y. Matsuoka. “Direct Neural Control of Anatomically Correct Robotic Hands.” In *Brain-Computer Interfaces*, edited by D.S. Tan and A. Nijholt, 105-19. Human-Computer Interaction Series. London: Springer, 2010.

Wiener, Norbert. *Cybernetics: Or Control and Communication in the Animal and the Machine*, second edition. Cambridge, Massachusetts: The MIT Press, 1961 (Quid Pro ebook edition for Kindle, 2015).

Wilkinson, Jeff, and Scott Hareland. “A cautionary tale of soft errors induced by SRAM packaging materials.” *IEEE Transactions on Device and Materials Reliability* 5, no. 3 (2005): 428-433.

Wiltshire, Travis J., Dustin C. Smith, and Joseph R. Keebler. “Cybernetic Teams: Towards the Implementation of Team Heuristics in HRI.” In *Virtual Augmented and Mixed Reality. Designing and Developing Augmented and Virtual Environments*, edited by Randall Shumaker, 321-30. Lecture Notes in Computer Science 8021. Springer Berlin Heidelberg, 2013.

Zamanian, Ali, and Cy Hardiman. “Electromagnetic radiation and human health: A review of sources and effects.” *High Frequency Electronics* 4, no. 3 (2005): 16-26.

Zarod, Marcin. “Constructing Hackers. Professional Biographies of Polish Hackers.” Digital Ecosystems. Digital Economy Lab, University of Warsaw, Warsaw, June 29, 2015.

Zebda, Abdelkader, S. Cosnier, J.-P. Alcaraz, M. Holzinger, A. Le Goff, C. Gondran, F. Boucher, F. Giroud, K. Gorgy, H. Lamraoui, and P. Cinquin. “Single glucose biofuel cells implanted in rats power electronic devices.” *Scientific Reports* 3, article 1516 (2013). doi:10.1038/srep01516.

Zhao, QiBin, LiQing Zhang, and Andrzej Cichocki. “EEG-Based Asynchronous BCI Control of a Car in 3D Virtual Reality Environments.” *Chinese Science Bulletin* 54, no. 1 (January 11, 2009): 78-87. doi:10.1007/s11434-008-0547-3.

*Chapter 4, "An Information Security Device Ontology for Advanced Neuroprosthetics,"*
*an excerpt from Gladden, Matthew E., The Handbook of Information Security for Advanced Neuroprosthetics,*
*ISBN 978-0-692-50161-0, Indianapolis: Synthypnion Academic, 2015, pp. 107-27.*

Zheng, Guanglou, Gengfa Fang, Mehmet Orgun, and Rajan Shankaran. "A Non-key based security scheme supporting emergency treatment of wireless implants." In *2014 IEEE International Conference on Communications (ICC)*, 647-52. IEEE, 2014.

Zheng, Guanglou, Gengfa Fang, Mehmet Orgun, Rajan Shankaran, and Eryk Dutkiewicz. "Securing wireless medical implants using an ECG-based secret data sharing scheme." In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, 373-77. IEEE, 2014.

Zheng, Guanglou, Gengfa Fang, Rajan Shankaran, Mehmet Orgun, and Eryk Dutkiewicz. "An ECG-based secret data sharing scheme supporting emergency treatment of Implantable Medical Devices." In *2014 International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 624-28. IEEE, 2014.