philosophies

MDPI

Article

Perspective and Boundary Exploration of Privacy Transfer Dilemma in Brain–Computer Interface—Dimension Based on Ethical Matrix

Tong-Kuo Zhang

School of Humanities, Dalian University of Technology, Dalian 116024, China; tongkuozh@mail.dlut.edu.cn

Abstract: The advent of intelligent technologies, notably Brain–Computer Interfaces (BCIs), has introduced novel privacy dilemmas. Ensuring judicious privacy transfer is imperative for the application of BCI technology and pivotal for fostering economic and technological progress. This study adopts privacy transfer as the research perspective and employs an ethical matrix as the research method. It establishes BCI users as the central core interests, with marketers, developers, and medical personnel as stakeholders. Departing from the binary opposition of public and private in traditional privacy theory, this article proposes ethical principles such as maximizing benefits, minimizing harm, and respecting independent decision-making power. It constructs a judgment matrix for the privacy transfer of BCIs, utilizing this matrix to identify ethical risks like privacy disclosure and hijacking. This study analyzes the reasons for risks, aiming to overcome dilemmas and construct an ethical matrix to explore privacy transfer boundary division methods suitable for BCI technology and tailored to different stakeholders.

Keywords: brain computer interface; ethical matrix; stakeholders; privacy transfer; privacy risk

Citation: Zhang, T.-K. Perspective and Boundary Exploration of Privacy Transfer Dilemma in Brain–Computer Interface—Dimension Based on Ethical Matrix. *Philosophies* **2024**, *9*, 10. https://doi.org/10.3390/philosophies9010010

Academic Editor: Marcin J. Schroeder

Received: 1 November 2023
Revised: 4 January 2024
Accepted: 5 January 2024
Published: 9 January 2024

1. Introduction

A typical Brain–Computer Interface (BCI) is a technology combining neuro-physiological measurements with machine learning software to detect brain activity patterns automatically [1]. BCIs apply neural data to other control systems by acquiring and translating them [2]. The neural data obtained by BCIs, commonly referred to as brain privacy, encompass concepts, memories, and thoughts observed from the brain [3]. Generally, privacy subjects have the right to decide to what extent their information can be disseminated to others [4]. However, in the use of brain–computer interfaces, especially in non-medical contexts, users, marketers, and developers may compromise their right to control privacy due to interest considerations, leading to excessive privacy transfer. Privacy transfer in BCIs refers to the need for users to transfer some of their privacy to effectively utilize the auxiliary functions of the BCI [5], obtaining a certain service [6]. At present, there is no analysis of the reasonable limit of privacy transfer in China. This article aims to explore the reasonable limit of privacy transfer through the method of an ethical matrix. The division of privacy transfer boundaries can achieve both privacy protection and privacy data sharing, enabling the use of transferred personal information for more valuable treatment, training, applications, and data research and development.

Reasonable privacy transfer cannot be achieved without appropriate ethical evaluation, and the ethical matrix provides a model for evaluating technical content. Building on the theoretical basis of the Mepham ethical matrix [7], this article establishes stakeholders and discusses the ethical dilemma in establishing privacy transfer boundaries by combining the technical characteristics of BCIs [8]. Finally, a targeted method for dividing privacy transfer boundaries is proposed. The ethics matrix includes a top-down expert-led model and a bottom-up comprehensive stakeholder evaluation model. This article mainly applies a bottom-up stakeholder evaluation model to ensure that numerous stakeholders can

participate in the discussion of the degree of privacy transfer in BCIs. Different stakeholders, while playing their respective roles, view the pros and cons of user privacy transfer from different perspectives. The ethics matrix can integrate the opinions of multiple stakeholders, including BCI users, marketers, developers, and healthcare professionals. In the early stage of the formation of the ethical matrix, it is set as a judgment matrix, which can identify the ethical issues in the process of BCI privacy transfer, namely the risks of privacy exposure and external environmental hijacking. By further analyzing the matrix to explore the root causes of ethical dilemmas, it is found that privacy paradoxes and technology worship can cause users to have vague concepts of privacy protection and become addicted to false needs, leading to the occurrence of ethical issues. Finally, an ethical matrix is established and a suitable method is found for dividing privacy transfer boundaries for BCI technology from the dimensions of various stakeholder roles.

2. Judgment Matrix: Revealing the Risk of Privacy Transfer

BCIs involve a diverse array of stakeholders. When delineating the ethical relationships among them, it is crucial to simplify and adjust, crafting a judgment matrix that aligns with the unique characteristics of BCI technology. Given that BCI users invariably occupy a vulnerable and central position in the technology's use, a BCI-user-centric approach is established, interlinking stakeholders such as marketers, developers, and medical teams to analyze the issue of unreasonable privacy transfer in BCI use.

2.1. The Lost Situation of Privacy Disclosure

While many BCI applications aim to enhance human quality of life, the inherent fragility and unstable signal characteristics of BCI technology may inadvertently leak users' brain signals, leading to an excessive transfer of user privacy. Furthermore, BCI users often lack awareness of privacy protection and possess weak privacy concepts, resulting in undue privacy transfer that jeopardizes their inner selves and seriously impacts their privacy and physical and mental health.

The fragility and instability of BCI technology's signal characteristics introduce vulnerabilities in information acquisition, processing, and decoding. This results in the forced disclosure of privacy, constituting passive privacy transfer. The human brain's neural signals are rich in electroencephalographic (EEG) information, containing a wealth of personal and private information. Brainwave information refers to the electrical signals of brain activity recorded through an electroencephalogram (EEG). An EEG is a non-invasive brain imaging technique that detects and records electrical activity in the brain's cortex by placing electrodes on the scalp. Brainwave signals reflect the synchronized discharges of neurons in the brain and are a common method used for studying brain function and diagnosing disorders of the nervous system [9]. Any monitoring or leakage of EEG information directly leads to the passive transfer of brain privacy, transforming private information into public knowledge. This not only violates the principles of "hidden" and "private" associated with privacy but also infringes upon human dignity and personal integrity [10]. Instances exist where brain spyware has been utilized to deduce a user's four-digit PIN, bank details, birth month, and place of residence [11]. Beyond objective information, hackers can eavesdrop on signals emitted by brain implants, [12] revealing emotions, biases, religious beliefs, and political inclinations [13].

Users exhibit varying perceptions of the value of privacy, coupled with weak control over their privacy, making comprehensive privacy guarantees challenging. Before employing BCI devices, users are typically required to read and agree to usage rules, which often go un-noticed. Research indicates that over 90% of consumers do not read the terms of service contracts they agree to [14]. Due to a lack of awareness regarding privacy protection, BCI users excessively surrender privacy. With evolving privacy concepts, "privacy" has transformed into a commodity, subject to calculation and weighing of pros and cons. Users tend to willingly surrender privacy in favor of perceived benefits, contributing to a proactive cession of privacy rather than its protection [15]. In BCI usage, the active transfer of

privacy is seen as facilitating more tailored services [16]. Consequently, BCI marketers and developers often prioritize market gains over ensuring consumers' willingness and ability to protect themselves [17]. For example, users grant marketers and developers extensive brain access rights to maintain timely BCI software updates. Patients using BCIs to control prosthetic limbs essentially "unload" their brains into the BCI system. The operational intricacies of BCIs remain independent and imperceptible, leaving users uncertain about the extent of information transfer and its utilization. Users may harbor suspicions that the device or external manipulation of their prosthetic limb is making incorrect decisions that could harm people [18]. BCI users are frequently willing to voluntarily relinquish privacy for training or research and development, sending sensitive brain data from the edge to the cloud for training [19].

Although current BCI applications focus on accessing narrow tasks or perceived brain signals, the rapid advancements in neurology and BCI technology suggest that BCI devices may eventually access more extensive brain signal data for a broader range of purposes. In such a scenario, determining users' control over their private information and the extent to which they can voluntarily relinquish privacy become challenging.

2.2. The Risk of Hijacking in the External Environment

The concept of a "cocoon room" arises from Cass Sunstein's "Information Utopia", describing the public's tendency to focus only on areas of personal interest, gradually becoming ensnared in a self-constructed "cocoon room" [20]. BCI's brain privacy reading technology can paint a more accurate self-awareness portrait than users' cognitive self-awareness. By recording every aspect of a user's life—what they eat, buy, read, see, and hear—BCI technology can depict emotions, fears, and happiness [21]. Future neural product companies may use obtained neural data and browsing traces to create personalized products tailored to individual preferences. These customized products function as self-built "cocoon rooms", entrapping users and providing a different kind of freedom through the consumption of tailored products. Some companies leverage users' neural characteristics to promote products beneficial to them, gradually solidifying thought patterns and stifling creativity and exploration of new ideas. Individuals become puppets manipulated by strings scattered throughout every corner of their brain.

BCI technology is even exploited to hijack users' brains through improper and covert means. Operators can stimulate the brain using high-frequency sounds inaudible to the user, influencing brain activity [22]. Such improper stimulation does not necessitate close interaction with users but can affect neural tissue, mental health, and psychological well-being. Effects may include emotional changes, depression, anxiety, or even suicidal thoughts [23]. Patients may unconsciously exhibit unwanted behaviors, such as gambling, unnecessary purchases, or criminal activities [24]. Attacks on neural stimuli can induce thoughts and behaviors in patients, leading to potential harm [25]. More concerning is the ease with which BCI users, hijacked by external technology, can become subservient to external influences [26].

3. Analytic Matrix: Exploring the Source of Privacy Transfer Dilemma

3.1. Paradox Problem: Ambiguous Attitude Leads to a Lack of Boundary Management

In the realm of BCI usage, the landscape of privacy and protection theory has undergone a paradigm shift. Privacy subjects find themselves not only in a unidirectional social environment but also within the multidimensional and dynamic digital context of BCIs. The challenge they face is the "privacy paradox": on one hand, concerns persist that less privacy transfer may yield insufficient benefits, while, on the other hand, technological and digital advancements necessitate relinquishing privacy for research or use convenience. The indifference of privacy subjects to the normalization of privacy transfer indicates a vague attitude towards privacy protection and a deficiency in managing the boundaries of privacy transfer.

The BCI, interconnected with users, transcends its role as a mere tool, evolving into a new living space intricately woven into users' existence. While BCI technology extends users' physical and psychological capacities, it concurrently engulfs them in the dystopia of technological monitoring and control. Concealed behind BCI's monitoring and control lies the assertion of new rights for stakeholders such as marketers, developers, and healthcare workers. User privacy data becomes a tool for these stakeholders to profit, as users' emotions, feelings, and activity traces are meticulously recorded and exploited [27]. The delineation of user privacy boundaries becomes increasingly blurred due to the emergence of new rights for stakeholders. This ambiguity arises from users' fluctuating attitudes toward privacy protection and their lack of awareness regarding privacy risks in the new technological environment. Additionally, there exists a gap between users' awareness of privacy protection and their ability to safeguard it.

The attitude towards privacy protection, reflecting one's subjective perception of information leakage, unauthorized access, and related outcomes, plays a pivotal role. A robust privacy protection attitude reinforces control over privacy boundaries, while a vague attitude lacks this control. The vagueness does not imply a lack of concern for privacy protection; rather, users, particularly in the field of BCI, exhibit a one-dimensional understanding of privacy [28]. They are unaware of the concealed risks in the new technological environment, characterized by a multidimensional and dynamic information context. This context emphasizes that information is no longer a mere collection of words but an inference within a specific setting. Appropriately acquiring information in relevant contexts constitutes reasonable privacy transfer; otherwise, it results in excessive privacy transfer. In the context of BCI treatment, for instance, a doctor acquiring clinical information from patients aligns with the principle of minimal rationality. However, obtaining unrelated information, such as emotions, beliefs, and habits, without user consent, for curiosity or research purposes, exceeds the boundaries of appropriate transfer. Users often waver between profit and privacy protection, especially when the perceived value of profit surpasses that of privacy. In such cases, users' attitudes toward privacy protection tend to become vague. Social Exchange Theory frames users' decisions to use BCIs as an exchange behavior, where consumers permit service providers to collect personal information for efficient services within manageable information risks. Users willingly exchange personal privacy data with economic value to obtain personalized services or other benefits. Users' unique privacy protection attitudes, formed by balancing benefits and risks, further influence their utilization of BCIs. Although service providers can collect conventional personal information, concerns arise when they delve into collecting biometric features, transaction data, etc. This raises apprehensions about potential privacy breaches, forming users' distinct privacy protection attitudes toward using BCIs, ultimately affecting the strength of control over privacy transfer boundaries.

The gap between privacy protection awareness and protection ability manifests as technology eroding the subject's autonomy in privacy decision-making. Users passively transfer privacy, relinquishing control over the transfer boundary, turning user privacy into a chain of interests for stakeholders. Different stakeholders benefit from this privacy interest chain based on their roles, with the primary victims being privacy subjects. Excessive privacy transfer typically occurs when users' personal privacy is disseminated to other stakeholders. Unlike traditional privacy transmission through interpersonal communication, considered "private" by privacy subjects, BCI technology, with its robust detection, processing, and storage capabilities, collects, saves, and tracks data easily. This may lead to privacy issues in terms of identifiability, monitoring, and security. Stakeholders can exploit stored data in the service provider's value chain, leading to potential theft by criminals and the use of information for extortion. Users, perceiving heightened security challenges to their personal privacy information, tend to resort to traditional methods of treatment and entertainment instead of accepting BCI's services.

3.2. Accelerated Sinking: Technology Worship Giving Rise to False Demands

The unique capacity of BCI technology to enhance sensory perception creates a mystique, tempting people to break away from existing norms or improve their quality of life. This allure increases users' fetishism towards BCI products, transforming them into socially worshipped entities [29]. This worship of digital technology results from the intrinsic value of digital technology and the influence of BCI stakeholders. The rationalization of technology leads people to believe it can bring about a leap in intelligence and physical fitness, positioning it as the sole pathway from necessity to freedom. While users may seem in control of technology, the underlying capital already exerts intangible manipulation over them. BCI technology, in a seemingly rational manner, turns users into puppets, eroding their autonomy. Enchanted by technology, users naturally become part of the social structure of BCI architecture. As BCIs permeate societal, consumer, and work trends, the resultant culture infiltrates various aspects of people's lives, subjecting their consciousness to constant monitoring by BCI stakeholders. People become perplexed, coerced, and subservient to the power of technology [30].

The enchantment with technology is not solely reflected in the evolution of technology worship but also in the reshaping process of BCI stakeholders using technology to mold user consumption habits and methods. BCIs manipulate and control users' consumption thoughts and behaviors by portraying individuals through neural data and covert nerve stimulation. This results in false demands that cater to the interests of other stakeholders. False demands involve consuming, entertaining, and acting according to advertising, aligning one's preferences with what others love or hate [31]. In BCI usage, privacy preferences are exploited to create information cocoons for users, promoting and endorsing specific products or inducing a shift in values and irrational consumption. The enchanting BCI technology seemingly crafts humans, turning users into homogeneous entities that are easily manageable. Under the dominion of BCI technology, the ontological characteristics of humanity gradually degenerate, leaving individuals in a perpetual quest for recognition. To demand recognition, individuals rely on technology, passionately consume, and feel immersed in a utopian world shaped by technology. Users are more inclined to accept visually appealing symbols, neglecting the reality beyond the illusory theater and becoming puppets manipulated by other stakeholders. The monopolization of privacy data dividends attracts stakeholders, encouraging them to induce users' attention and consumption by fabricating false demands. Stakeholders exploit collected user privacy data, transforming it into symbolic illusions that create a false sense of prosperity tailored to users, fostering addiction. Users mistakenly believe they are gaining leisure, but this is essentially the exploitation and new enslavement of their remaining labor time by technology. The illusion is that only through consumption can one experience leisure. Users privately assume they exchange consumption for freedom, yet this freedom makes self-control more challenging. In the material world, individuals blindly seek identification, even without knowing who they are and why they exist. They lose control over their freedom, and only through controlling desires with reason and passion can they achieve the management of harmonious consciousness—that is, the rational transfer of private data. The BCI is a complex technology requiring collaboration across various teams from design to research and development, production, and sales. When users experience BCI products, the relationship chain between stakeholders behind these products remains hidden within the products. The illicit collection and sales relationship chain of user privacy is unknown, posing not just a hidden risk of BCIs but a common challenge faced by cutting-edge technology today.

4. Ethical Matrix: Illustrating the Boundaries of Privacy Transfer

Establishing privacy transfer boundaries within BCIs revolves around meeting the needs of both BCI users and other stakeholders. A reasonable boundary of privacy transfer should have a protective mechanism to maximize the interests of all stakeholders, fulfill fundamental demands, and allow each stakeholder to obtain the privacy they need. Additionally, it should mitigate the harm of excessive privacy transfer to minimize the negative

impact. Establishing a reasonable privacy transfer boundary is contingent upon BCI users possessing a clear attitude towards privacy protection and independent decision-making power. Simultaneously, other stakeholders should respect the control rights of privacy owners over their privacy. The ethical principles of the BCI privacy transfer ethics matrix (Table 1) specifically embody maximizing benefits, minimizing harm, and respecting the right to independent decision-making.

Table 1. Ethical matrix for privacy transfer.

Interest Groups	Maximum Benefit	Minimize Hazards	Respect for Autonomy in Decision-Making	Method of Establishing Boundaries
BCI Users	Precision therapy Comfortable experience	Privacy is controllable	Freedom and privacy transfer	Clarify privacy protection attitude Privacy decision-making power
Marketer	Highly acclaimed products and services	Collect user experience to upgrade products	Autonomous marketing	Transparent data flow The gentle right to be forgotten [11]
Developer	Promoting technological innovation	Obtain privacy data available for development	Independent research and development	Jointly building a privacy sharing database The balance between development and privacy protection
Medical Personnel	Precision therapy	Users do not resist BCI treatment mode	Autonomous diagnosis and treatment	Avoiding information leakage outside of the scenario Establishing an appropriate informed consent model

Analyzing the risks associated with BCI privacy transfer reveals the intricate nature of establishing privacy boundaries. A comprehensive understanding of potential privacy risks is crucial considering the diverse range of stakeholders involved. BCI users often lack clarity regarding the purpose of privacy, maintain vague attitudes toward privacy protection, and possess insufficient decision-making rights. Marketers, seeking to spur economic development and cater to entertainment needs, strive to access partial user privacy. Developers rely on privacy data for ongoing BCI software development and enhancement, while medical personnel require privacy information for effective treatment. Guided by principles of seeking benefits, avoiding harm, respecting autonomy, and ensuring fairness and justice, a targeted approach for delineating privacy transfer boundaries is proposed for distinct stakeholders within the BCI domain.

Firstly, Establishing Privacy Transfer Boundaries for Users. Initiating the construction of privacy transfer boundaries for BCI users demands a resolute and clear stance on privacy protection. Users must recognize privacy as a highly valuable, multidimensional entity, extending beyond a focus on one-way privacy information. Failing to grasp privacy information holistically and undervaluing privacy when weighing benefits and risks facilitate easy privacy transfer. Respecting users' independent decision-making rights is paramount. Transparent privacy management methods and usage regulations should be established, enabling BCI users to easily access and monitor transferred privacy within a controllable range. Transparent privacy management facilitates privacy sharing and caters to the privacy needs of other stakeholders. As Sandra Petronio highlights in her "Communication Boundary Management Theory," the free flow of information depends on the opening and closing of boundaries [32]. Consequently, the degree of user privacy openness and sharing should be determined by the privacy owner, mitigating instances of other stakeholders forcibly seizing and distorting appearances to obtain user privacy.

Secondly, Constructing Privacy Transfer Boundaries for Marketers. While the commercial use of privacy is advantageous for customizing users' entertainment needs, the

transitional customization of information may lead to information silos and homogenization. To establish privacy transfer boundaries for BCI entertainment products, it is imperative to institute a robust privacy business management system. This involves effective connections between relevant legal regulatory departments, bridging business and law to avoid privacy management loopholes. Additionally, tracing the usage path of privacy information; emphasizing the importance of preventing the sale and theft of privacy information; and establishing a visible, perceptible, and controllable privacy business management mechanism are crucial. Advocating for a "moderate right to be forgotten," which promotes a restricted and non-abusive right to be forgotten, helps avoid hindering economic development. Simultaneously, active advocacy for the construction of codes of conduct and technical standards ensures a balance between data development and utilization and data rights protection, without outright deletion [11].

Thirdly, Establishing Privacy Transfer Boundaries for Developers. The establishment of privacy transfer boundaries for developers involves joint efforts in building a privacy-sharing database while balancing BCI development with privacy protection. Privacy information from users offers numerous benefits to developers, particularly in the realms of entertainment and technological innovation. To achieve this, users must understand the benefits of privacy transfer for a robust healthcare system. Reasonable compensation mechanisms should be provided for users engaging in privacy transfer. Privacy owners, utilized for data analysis, should be able to track access through improvements to the database management model. Adapting to the group characteristics of BCI users involves guiding users to reasonably transfer privacy through educational and encouragement mechanisms. Jointly building a private shared database ensures mutual benefit.

Fourthly, Exploring Privacy Transfer Boundaries for Medical Personnel. Effective and reasonable privacy transfer is crucial for the precise treatment of BCI patients. However, insufficient understanding and trust in BCI technology often result in inadequate privacy transfer by users, hindering reasonable and effective treatment. The exploration of privacy transfer boundaries for medical personnel should commence with efforts to improve the popularity of BCI technology. Focus on users with insufficient understanding abilities is key to technology popularization. Abandoning the traditional doctor–patient relationship model in favor of a manager–technical trust mechanism for equal dialogue is essential. Optimizing informed consent based on technology popularization is crucial to help BCI users understand the risks of insufficient privacy transfer and the advantages of reasonable privacy transfer for treatment. Additionally, establishing a compliant privacy data management mechanism is vital to prevent user data overflow beyond the context, safeguarding it from theft and abuse by illegal entities.

5. Conclusions

The transformative force demonstrated by Brain–Computer Interface (BCI) technology compels us towards it. As this technology flourishes, one should not be deceived by its brilliance and eagerly trade the most precious privacy for false needs. Improper use of technology is perilous as it can dominate, enslave, and alienate people. Simultaneously, technology is also secure as it can rejuvenate us and bring about changes in our production and lifestyle. As stewards of technological discourse, we should not suppress or exclude technology but rather achieve self-awareness of technology, return to rationality, and avoid the worship of science and technology.

As an emerging intelligent technology, the Brain–Computer Interface (BCI) is no longer suitable for seeking the manifestation of privacy boundaries through the traditional public–private binary opposition model. The bottom-up multistakeholder perspective of the ethics matrix not only avoids multidimensional privacy risks when using BCI technology but also provides concrete theoretical and practical references for the development of BCIs. In addition to the vague attitude towards user privacy mentioned in the article, as well as the lack of privacy decision-making power caused by the manipulation of privacy by technological domination, factors such as cultural value orientation and new diverse

subjects may lead to the occurrence of privacy risk issues such as excessive privacy selling, privacy theft, and hijacking by users. Further discussion of these issues not only contributes to the healthy development of technology and protects individual privacy interests of users, but also promotes information security in society, enhances technological trust, and seeks development for the overall welfare of humanity.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data policy compliant with NRR.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Gerven, M.V.; Farquhar, J.; Schaefer, R.; Vlek, R.; Geuze, J.; Nijholt, A.; Ramsey, N.; Haselager, P.; Vuurpijl, L.; Gielen, S.; et al. The Brain–Computer Interface Cycle. *J. Neural Eng.* **2009**, *6*, 041001. [CrossRef] [PubMed]
2. Allison, B.Z.; Wolpaw, E.W.; Wolpaw, J.R. Brain-computer interface systems: Progress and prospects. *Expert Rev. Med. Devices* **2007**, *4*, 463–474. [CrossRef] [PubMed]
3. Stepke, F.L. CLAUSEN, JENS & LEVY, NEIL (editors) Handbook of Neuroethics. *Acta Bioethica* **2015**, *21*, 150.
4. Warren, S.D.; Brandeis, L.D. The Right to Privacy. *Harv. Law Rev.* **1890**, *4*, 193–220. [CrossRef]
5. Xiao, F. Ethical challenges and principles to be followed in brain computer interface technology. *Acad. J. Zhongzhou* **2022**, 95–102.
6. Liu, G.; Wang, J. Research on the Use of Personal Information and Privacy Transfer in Digital Epidemic Prevention. *Youth Joumalist* **2021**, 87–89.
7. Mepham, B.A. Framework for the Ethical Analysis of Novel Foods: The Ethical Matrix. *J. Agric. Environ. Ethics* **2000**, *12*, 165–176. [CrossRef]
8. Forsberg, E.M. Pluralism, The Ethical Matrix, and Coming to Conclusions. *J. Agric. Environ. Ethics* **2007**, *20*, 455–468. [CrossRef]
9. Poldrack, R.A.; Monahan, J.; Imrey, P.B.; Reyna, V.; Raichle, M.E.; Faigman, D..; Buckholtz, J.W. Predicting Violent Behavior: What Can Neuroscience Add? *J. Trends Cogn. Sci.* **2017**, *22*, 111–123. [CrossRef] [PubMed]
10. Yang, Z. On the Innovation of Privacy Ethics Based on Contextual Integrity in the Context of Big Data Monitoring. *Study Pract.* **2020**, 128–134.
11. Martinovic, I.; Davies, D.; Frank, M.; Perito, D.; Ros, T.; Song, D. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In Proceedings of the Security'12: Proceedings of the 21st USENIX Conference on Security Symposium, Bellevue, WA, USA, 8–10 August 2012; USENIX Association: Berkeley, CA, USA, 2012.
12. Lenca, M.; Haselager, P. Hacking the brain: Brain–computer interfacing technology and the ethics of neurocircuitry. *Ethics Inf. Technol.* **2016**, *18*, 1–13.
13. Bonaci, T.; Calo, R.; Chizeck, H. App Stores for the Brain: Privacy and Security in Brain-Computer Interfaces. In Proceedings of the 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, Chicago, IL, USA, 23–24 May 2014; IEEE Press: Piscataway, NJ, USA, 2014.
14. Guynn, J. What You Need to Know before Clicking "I Agree" on That Terms of Service Agreement. *TechXplore*, 29 January 2020. 29 January.
15. Zhang, X.; Tian, X. Research on the Path of the Privacy Paradox of Mobile Social Media Users: An Empirical Analysis Based on fsQCA. *Inf. Stud. Theory Appl.* **2020**, 92–97.
16. Liu, Y.; Zhang, T.; Jin, X.; Cheng, X. Personal Privacy Protection in the Era of Big Data. *J. Comput. Res. Dev.* **2015**, *52*, 229–247.
17. Bailey, R.; Schleiter, K.E. Testing Manufacturer Liability in FDA-Approved Device Malfunction. *Virtual Mentor* **2010**, *12*, 800–803.
18. Reilly, C.M. Brain–Machine Interfaces as Commodities: Exchanging Mind for Matter. *Linacre Q.* **2020**, *87*, 387–398. [CrossRef] [PubMed]
19. Li, H.; Chen, H.; Xu, C.; Das, A.; Chen, X.; Li, Z.; Xiao, J.; Huang, M.-C.; Xu, W. Privacy computing using deep compression learning techniques for neural decoding. *Smart Health* **2022**, *23*, 100229. [CrossRef]
20. Sangstein, K. *Information Utopia: How People Generate Knowledge*; Bi, J., Translator; Law Press: Beijing, China, 2008.
21. Lukacher, N.; Zizek, S. Incontinence of the Void: Economico-philosophical Spandrels. *CHOICE Curr. Rev. Acad. Libr.* **2018**, *55*, 1214.
22. Fukushima, A.; Yagi, R.; Kawai, N.; Honda, M.; Nishina, E.; Oohashi, T. Frequencies of Inaudible High-Frequency Sounds Differentially Affect Brain Activity: Positive and Negative Hypersonic Effects. *PLoS ONE* **2014**, *9*, e95464. [CrossRef]
23. Musk, E.; Neuralink, S.H. An integrated brain-machine interface platform with thousands of channels. *J. Med. Internet Res.* **2019**, *21*, e16194. [CrossRef]
24. Pycroft, L.; Boccard, S.G.; Owen, S.L.F.; Stein, J.F.; Fitzgerald, J.J.; Green, A.L.; Aziz, T.Z. Brain jacking: Implant Security Issues in Invasive Neuromodulation. *J. World Neurosurg.* **2016**, *92*, 454–462. [CrossRef]

25. Marin, E.; Singelée, D.; Yang, B.; Volski, V.; Vandenbosch, G.A.E.; Nuttin, B. Bart Preneel Securing Wireless Neurostimulators. In Proceedings of the Eighth ACM Conference, Tempe, AZ, USA, 19–21 March 2018; ACM: New York, NY, USA, 2018.
26. Decew, J.W. In pursuit of privacy: Law, ethics, and the rise of technology. *J. Ethics* **1999**, *109*, 402–406.
27. Fuchs, C.; Mosco, V. *The Return of Marx*; Communication Station Workshop, Translator; East China Normal University Press: Shanghai, China, 2017; pp. 418–419.
28. Ali, S.S.; Lifshitz, M.; Raz, A. Empirical Neuroenchantment: From Reading Minds to Thinking Critically. *Front. Hum. Neurosci.* **2014**, *8*, 357. [CrossRef] [PubMed]
29. Marx, K. *Das Kapital*; Zhu, D., Translator; Jiangsu People's Publishing House: Nanjing, China, 2013.
30. Zhang, A.; Wang, F. The political security risks of "big data killing". *Future Commun.* **2021**, 48.
31. Marcuse, H. *Unidirectional People: A Study on the Ideology of Developed Industrial Society*; Zhang, F., Lv, S., Translators; Chongqing Publishing House: Chongqing, China, 1988; p. 6.
32. Petronio, S. Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples. *Commun. Theory* **1991**, *1*, 311–335. [CrossRef]