Original Article:

Privacy, surveillance, and implanting RFID microchips to humans*

Tayyibe Bardakçı

Abstract:

Background: Radio Frequency Identification (RFID) technology is specifically designed for the remote identification of objects. The first patent for human implantable RFID microchips was granted in 1997, and the FDA approved these microchips in 2004. Since then, they have found applications in humans for diverse reasons. ***Objective:*** This study aims to make an ethical evaluation of using RFID microchips in humans, focusing on privacy and surveillance. ***Methods:*** A literature review was conducted, exploring the conceptual dimensions of privacy and surveillance, and ethical evaluations were made regarding potential privacy violations caused by RFID microchips, as well as their potential uses for surveillance purposes. ***Results:*** Privacy is a multidimensional concept that spans various disciplines such as psychology, sociology, anthropology, medicine, theology, and law, and throughout history it constitutes an indispensable and intrinsic necessity for humanity. On the other hand, surveillance is a process wherein certain groups employ methods to gather, accumulate, analyze, process, and utilize data, with the objective of regulating the behavior of specific groups, entailing potential physical, ideological, or structural interventions, ultimately aiming to guide individuals toward predetermined behavioral patterns. ***Discussion and Conclusion:*** A major concern with RFID microchips is potential privacy violations and their use for surveillance. These microchips and their connected networks hold a significant amount of information, including sensitive data like health-related information. Thus, they make individuals become easily identifiable and make them vulnerable to surveillance practices.

Keywords: Ethical concerns, microchip implant, privacy, RFID, surveillance.

International Journal of Human and Health Sciences Vol. 08 No. 01 January'24
DOI: http://dx.doi.org/10.31344/ijhhs.v8i1.626

Introduction

In recent years, various technologies including but not limited to identification cards, passports, smartphones, city surveillance cameras, and facial recognition technologies at airports, have increased surveillance to higher levels than ever before. However, a microchip implanted in humans, due to its invasive nature, makes surveillance more pervasive. Particularly, microchips containing radio frequency identification technology, makes surveillance possible at every moment of our lives.

Radio Frequency Identification (RFID) represents a technology explicitly engineered for the remote identification of objects. RFID tags function by transmitting unique identification numbers to electronic readers through the utilization of radio waves.[1] The RFID microchips, typically comparable in size to a grain of rice, are categorized into three principal types: passive, active, and semi-passive. Passive microchips operate without an internal power source, whereas active microchips possess an independent power source, typically manifested in the form of a small battery. Conversely, semi-passive microchips, also recognized as battery-assisted RFIDs, remain dormant until activated by a signal from the interrogator. Although active RFIDs exhibit a prolonged read range and larger memory capacity, passive RFIDs endure for extended durations

* This article is based on the PhD thesis titled "Ethical Evaluation of Implantable Enhancement Technologies," which was conducted at Istanbul University, Graduate School of Health Sciences.

Correspondence to: Tayyibe Bardakçı, Istinye University, Medical Faculty, Department of Deontology and Medical History; Istanbul University, Graduate School of Health Sciences, Istanbul, Turkey. E-mail: tayyibe.b@gmail.com

as they function without reliance on batteries.[2] Notably, contemporary microchips predominantly employed are of the passive classification.

The application of RFID microchips on animals has been implemented in numerous countries globally over an extended period. In Türkiye, a recent legislative mandate has made it obligatory to implant microchips in pets.[3] The reason for the use of these microchips in domestic animals is primarily the easy identification of animals and thus the ability to find the owners of lost animals. Furthermore, these microchips are designed to store vaccination details and health records, making it more convenient to provide medical care to animals.[4]

The initial patent for human implantable RFID microchips was granted in 1997, and subsequent to that, the United States Food and Drug Administration (FDA) accorded approval to *VeriChip*'s RFID microchips in 2004, categorizing them as a class II medical device. The *VeriChip* device is specifically designed to facilitate the identification of patients and the storage of their medical histories on microchips, thereby enabling healthcare personnel to access pertinent information as required.[5,6]

One of the first examples of the use of RFID microchips on a human being was an experiment conducted by Kevin Warwick in 1998. The motivation behind this experiment, framed within the context of Warwick's quest to intimately engage with technology, entailed his deliberate integration with the computer network within the designated building. This integration enabled the meticulous tracking of Warwick's movements, including spatial parameters such as his locations within the building, the specific rooms visited, and the duration of his presence in each room. A noteworthy outcome of Warwick's experiment was how quickly he came to feel that the implant was a natural part of his body. Later, when prompted to remove the implant due to the potential side effects, Warwick reported a strong emotional reaction, describing it as similar to the feeling of losing a close friend. This highlights the deep psychological impact of the implantation experience.[7]

The substantive focus and media coverage surrounding microchips gained considerable momentum in 2015, concomitant with the initiation of microchip implantation initiatives by certain companies. Notably, *Epicenter* in Sweden led this trend by implanting microchips in 150 employees in the inaugural instance. Following this trend, *Three Square Market* in the United States embraced microchip implantation two years later, incorporating it into their company and even organizing office events to facilitate the procedure. In Belgium, *New Fusion* similarly adopted the integration of RFID microchips, marking another instance of such implementations among employees in the same year. A broader examination of similar cases in countries like the United Kingdom and Germany indicates a noticeable global increase in microchip implants.[8-10]

Exploring the benefits of RFID microchips, exemplified by the FDA-approved *VeriChip*, reveals their usefulness in the medical field. Many individuals choose to have these microchips for medical purposes, allowing them to store their complete medical histories on the microchip. This integration renders patients' crucial medical information readily accessible to healthcare professionals, particularly in emergency scenarios when patients are admitted to hospitals. The effectiveness of such microchips is particularly notable when patients are unable to communicate or are unconscious, and family members are not present.[11] This capability was highlighted by a significant incident in 2006, representing the first documented case of a life-saving intervention facilitated by an RFID microchip implant. In this case, medical practitioners successfully accessed the patient's medical records from the embedded database through the microchip, thereby contributing to the preservation of the patient's life following an accidental head injury.[12]

Furthermore, in the context of conditions such as dementia, Alzheimer's disease, or mental disorders, the implantation of RFID microchips can be used in enhancing patient monitoring. Such microchips, when implanted in individuals grappling with these conditions, facilitate the timely notification of caregivers or medical practitioners when patients go outside their home or medical facility. Proponents also suggest that employing these microchips in newborns and young children could act as a preventive measure against the risks of abduction and disappearance, adding an extra layer of security for this vulnerable demographic.[13]

RFID microchips can also store information about

an individual's preferences for end-of-life medical decisions.[14] This includes the incorporation of "advance directives," a term within the purview of medical ethics covering documents such as "living will," "durable power of attorney," or "do not resuscitate" (DNR) orders. Such directives can be digitally stored on these microchips, providing a convenient and easily accessible record of an individual's expressed medical preferences.

An interesting application of RFID implants is in the realm of security. Specifically, some institutions have adopted the practice of implanting microchips in authorized personnel who need access to secure areas with strict security measures. For example, a company based in Ohio/U.S. implanting microchips in employees granted access to restricted areas. Similarly, the Ministry of Justice in Mexico has integrated microchips into 18 of its personnel.[14]

Apart from the mentioned uses, people choose microchip implants as a means of enhancing convenience and expediency in both their daily lives and professional environments. For example, many people usually carry multiple items like ID cards, driver's licenses, or credit cards in their wallets. However, these physical documents can be easily lost, stolen, or misplaced. In modern times, using microchip implants as alternatives to traditional documents helps minimize these risks, providing a quicker and more secure way to access information without the concerns of forgetfulness or theft. In office environments, integrating microchips serves various purposes, such as providing secure access to offices and computer systems, as well as operating office equipment like printers and copiers.[12,13]

Methods

This study undertakes an ethical evaluation of using RFID microchips in humans, focusing on the fundamental concepts of privacy and surveillance. To achieve this objective, we conducted a literature review delving into the conceptual dimensions of 'privacy' and 'surveillance'. Then we analyzed how these concepts are addressed in the academic literature and made ethical evaluations pertaining to potential privacy violations caused by RFID microchips, as well as their potential uses for surveillance purposes.

Results

What is privacy?

Privacy is a multidimensional concept that spans various disciplines such as psychology, sociology, anthropology, medicine, theology and law. There is some information that, in some primitive societies, a distinctive practice emerged wherein individuals, seeking solitude, would turn their faces to walls, effectively signifying an aspiration for uninterrupted personal space within the family members. Looking back at ancient civilizations like ancient Egypt and Rome, we see that having the privilege of privacy was a clear sign of high status. Notably, individuals of elevated societal standing demonstrated their status through the utilization of spatial environments characterized by high entrances and enclosed spaces.[15] Within these socio-cultural frameworks, wherein human dignity is inextricably linked to one's status, the correlation between privacy and privilege becomes apparent.

The concept of privacy, which is sometimes associated with a sense of shame, is also found in anthropological and religious sources.[16] Within anthropological studies, feeling of shame, perceived as unique to humans among living entities, traces its origins back to primitive societies.[17] Religious sources, exemplified by the narratives of Adam and Eve in both the Torah and the Qur'an, illustrate the intrinsic human inclination towards privacy and shame, as evidenced by their subsequent attempts to conceal their nudity following the consumption of the forbidden fruit.[18,19] The Quranic injunction against entering others' homes without permission also shows the significance accorded to privacy within the Islamic framework.[20]

In the scholarly literature about privacy, significant insights have been offered, notably by American jurists Warren and Brandeis in their well-known 1890 article, "The Right to Privacy".[21] Their formulation characterizes privacy as "the right to be alone," emphasizing the entitlement to a personal sphere or sanctuary. Subsequently, Alan Westin, in his 1967 publication "Privacy and Freedom," provided an expanded definition, conceptualizing privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Westin posited privacy within an individual's social context as a "voluntary and temporary" withdrawal from

society, achievable through mechanisms such as solitude, intimate association with small groups, or the maintenance of anonymity or secrecy in larger gatherings.[16,22] This influential definition by Westin places paramount emphasis on the right to exert control over one's information. Moreover, his conceptualization of privacy extends beyond the individual to include group privacy, especially within interpersonal relationships, recognizing the collective dimensions of privacy.

Irwin Altman, another significant figure in privacy studies, defined privacy as "the selective control of access to oneself." Altman explains this idea using the concept of boundary control, where individuals alternately expose themselves to others and, at other times, seclude themselves.[23] Altman's perspective presents privacy as a nuanced balance of personal preferences. It suggests that individuals, moving between moments of solitude and social interaction, actively manage the selective control of access to different aspects of their identity.

Richard Parker contributes to the discussion on privacy by framing it as "the control of when and by whom various parts of us can be perceived." The utilization of the term "perceive" in this context is deliberate, including not only visual observation but also other senses like hearing, touching, smelling, and tasting. The phrase "parts of us" within this definition covers visible aspects of our physical appearance, vocal expressions, and nearby belongings, which can include things like hair, bodily fluids, and personal items, particularly relevant in medical and clinical situations.[24] While the initial thought might be to link this definition mainly with physical body components, it's crucial to recognize the contemporary expansion of privacy considerations. This includes personal communication and controlling access to possessions like mobile phones, protected by passwords to prevent unauthorized access.[24] This broader perspective emphasizes the diverse nature of privacy, going beyond traditional boundaries to include a range of personal elements and belongings that individuals aim to control access to in today's contexts.

In the examination of privacy paradigms, scholars often categorize it into three main types: personal, spatial, and informational privacy. Personal privacy is construed as a safeguard against unwarranted intrusions upon an individual, particularly in the contexts of surveillance and physical contact. Spatial privacy, on the other hand, involves maintaining the privacy of the physical space surrounding an individual. Information privacy, which is on our agenda more and more today with the increasing amount of data generated by digital technologies, is to keep the control of our own information in our hands.[25]

In addition to this, Roger Clarke (1997) represents a comprehensive taxonomy of privacy, categorizing it into four distinct domains: personal privacy, personal behavior privacy, personal communication privacy, and personal data privacy. The first domain, often referred to as "body privacy," pertains to the inviolability of the physical body. Instances falling within this purview include unauthorized medical interventions such as compulsory vaccinations, non-consensual blood transfusions, or mandatory sterilization. Personal behavior privacy covers a broad spectrum of conduct, with particular emphasis on sensitive matters such as religious practices, sexual behaviors, or political activities. Personal communication privacy aims to protect the free exchange of information through various means from surveillance or eavesdropping. Lastly, personal data privacy ensures that one's data remains inaccessible to unauthorized entities, giving individuals significant control over the dissemination and use of such information.[26]

On the other hand, Finn et al. argue that Clarke's four-category classification of privacy falls short considering recent advances in biotechnology and information and communication technologies. Introducing a more detailed framework, they propose seven distinct categories to better address privacy considerations:[27] Privacy of the person, privacy of behavior and action, privacy of communication, privacy of data and images, privacy of thoughts and feelings, privacy of location and space, and privacy of community.

In summary, the conceptualization of privacy exhibits variability across diverse societies and cultures, and its understanding can change over time even within the same society. Nonetheless, irrespective of the evolving definitions and parameters of privacy, there exists a common acknowledgment across cultures throughout history that privacy constitutes an indispensable and intrinsic necessity for humanity.

What is surveillance?

Another concept closely linked to privacy is surveillance. Primarily examined from a sociological perspective, surveillance is described as a complex process where certain entities use methods to gather, accumulate, analyze, process, evaluate, and use data. The goal is to regulate the behavior of specific groups, involving the potential for physical, ideological, or structural interventions. In essence, surveillance aims to guide individuals toward predetermined behavioral patterns.[28]

From a historical perspective, the origins of surveillance practices can be traced to the introduction of writing. According to Anthony Giddens, the introduction of written texts facilitated the classification and definition of individuals and events, marking a pivotal development in the capacity to document and categorize.[29] The practice of recording events, such as censuses or the enumeration of military forces, had a profound impact on societal functioning, strengthening the authority of states. A notable example is the "Domesday Book," commissioned by the Kingdom of England in the 11th century, which meticulously recorded information about lands and incomes of the population.[30] This systematic archiving of data played a key role in enhancing the power of governing entities. The subsequent advent of the printing press, conversely, not only facilitated the practicalities of recording and reproducing written texts but also emerged as a consequential instrument that further solidified the authority wielded by states.[29]

Within the field of surveillance literature, Karl Marx emerges as a key figure to systematically engage with the conceptual underpinnings of surveillance. According to Marx, surveillance plays a crucial role in capitalist societies, functioning as an essential tool for boosting production. Capital owners are driven by the need to extract more surplus-value while minimizing costs, and this goal is achieved through careful monitoring of the working class. Thus, factories serve not only as places of production but also as mechanisms of oppression designed to reshape the proletariat.[31,32] In this system, where workers appear to be free in form, there is no need for the employer to discipline the worker by force. Nevertheless, the worker, subjected to constant surveillance by the employer and reliant solely on this employment for sustenance, is compelled to intensify labor efforts and self-discipline to enhance productivity within defined temporal constraints. In fact, factories that gather workers under the same roof, optimize the oversight of the entire workforce and concomitantly increase overall productivity.[33]

Max Weber, a distinguished sociologist, also recognizes the influence of capitalist systems on surveillance, offering a perspective distinct from Karl Marx's. Weber argues that surveillance practices go beyond class relations and are closely connected to bureaucratic structures. Within contemporary institutions, a highly organized hierarchical system of salaried employees systematically documents all aspects of operations, yielding not only heightened operational efficiency but also facilitating a form of social control. In these bureaucratic settings, there is a noticeable boost in managerial confidence regarding the thorough implementation of directives, illustrating the interconnectedness of surveillance, bureaucracy, and managerial authority.[33]

Michel Foucault, a pivotal figure in surveillance studies, characterizes contemporary societies as "disciplinary societies." Foucault's conceptualization of surveillance extends beyond the confines of the traditional worker-employer dynamic or bureaucratic structures, permeating the entirety of modern societal frameworks. In contemporary contexts, surveillance practices have evolved from direct oversight, as seen in historical instances, to an indirect manifestation facilitated through mechanisms of "confinement." Foucault introduces the notion of the "panopticon," an architectural design conceptualized by Bentham in the 18th century for the systematic surveillance of individuals, such as prisoners in jails. Employing the panopticon as a metaphor, Foucault explains how power structures have pervasive authority over society.[34,35]

Within this conceptual framework, Foucault uses the panopticon metaphor to illustrate power dynamics. Instead of the traditional visible authority like a monarch delivering punishments, there's an "invisible power" at play. This unseen authority necessitates individuals to constantly monitor themselves. According to Foucault, the panopticon establishes "a state of conscious and continuous visibility that ensures the automatic functioning of power." Instances such as hospitals, schools, or prisons, symbols of the panopticon model, are characterized by the omnipresence of this invisible power, exerting control by confining

individuals within these institutional structures.[34] Consequently, within this paradigm, patients willingly acquiesce to medical treatment, students conform to school regulations, and prisoners refrain from disruptive behavior.

At this point, it is pertinent to mention the concept of "biopower" used by Foucault to explain the control over lives and bodies. Within the framework of capitalist systems, Foucault posits regulating bodies becomes crucial to maximize productivity and ensure compliance with work-related rules. This means focusing on improving the capabilities of bodies, enhancing their functionality, and aligning them with economic demands. In the era of biopower, the objective is twofold: not just strengthening bodies through investment, avoiding the need for outdated disciplinary methods like lethal measures or punishments, but also enforcing obedience through various power strategies, essentially turning these bodies into mechanized entities. It is noteworthy that, despite the apparent emphasis on physical intervention, the ultimate aim of biopower is to shape consciousness in accordance with its principles. The main focus of biopower is to nurture compliant bodies that adhere to established norms, avoid deviation, and undergo a process of pacification.[36]

To establish and maintain control, certain organized mechanisms are necessary. According to Foucault, specific institutions such as schools, barracks, monasteries, hospitals, and prisons are strategically positioned to regulate societies effectively, facilitating the shaping of compliant individuals. Furthermore, the quantification and evaluation of bodies undergoing these regulatory processes involve using medical methods as essential tools in the pursuit of societal 'normalization'.[36] In the context of biopower, individuals take responsibility for their own actions, aiming to fit into societal expectations to gain acceptance. This requires a conscious effort to regulate behavior, ensuring alignment with established norms and avoiding deviations. Essentially, people internalize the principles of discipline, allowing the influence of power to extend into various aspects of their lives.

In 1985, sociologist Gary T. Marx introduced the term "surveillance society" in his article, "Surveillance Society: The Threat of 1984-Style Techniques".[37] In his work, Marx highlighted a significant change in surveillance, driven by advancements in computer technologies. Nowadays, these technologies have the ability to infiltrate not only our physical and social spaces but also our personal lives. What's noteworthy is that these new surveillance tools allow for widespread monitoring, targeting entire societies rather than just specific individuals. This shift in surveillance has serious implications. Governments can use these advanced technologies to surveil various groups, such as ethnic or religious minorities, or anyone perceived as different from societal norms. Complicating matters is the fact that these surveillance technologies are often difficult to detect, making it even more challenging to safeguard our privacy.[37]

Likewise, David Lyon, in reference to the capabilities of emerging microelectronics-based technologies for storing and processing more intricate information, argues that individuals' data is becoming progressively more accessible. Entities employing surveillance technologies can readily obtain access to various aspects of people's lives, including financial information, health records, residential details, and telephone communications. In essence, the capacity for surveillance is expanding continuously with the advent of new technologies.[33]

In addition to the aforementioned considerations, the advent of novel technologies has brought about a paradigmatic shift within the panopticon metaphor. One example of this shift is seen in the 'synopticon' model, which emerged in the early 20th century as a response to the advent of television and other mass media. Developed by Thomas Mathiesen in 1997, this conceptual framework deviates from the traditional panoptic model where a select group in positions of authority observes the majority. Surveillance in the synopticon relies on the relational bond between the majority and the televised minority whether fictional or real. Through this connection, those in power can subtly influence the majority without resorting to coercion, controlling and disciplining through mediated messages.[38,39] Zygmunt Bauman captures this shift by stating, "The panopticon forced people into a position where they could be watched, while the synopticon does not need coercion; it seduces people to watch".[40] In summary, in the synopticon framework, admiration for individuals on the screen leads to the homogenization of individuals, guided by the influence of power. Under the impact of synoptic

surveillance, individuals develop shared cognitive patterns and readily conform to the prevailing societal system.

Developments in computer technologies in the second half of the twentieth century led to the development of the 'superpanopticon' model of surveillance. This concept, developed by Mark Poster, refers to the fact that with the development of computers' ability to obtain and store information, it has become possible to silently and continuously monitor large numbers of people. In the superpanopticon, many daily activities such as our shopping patterns, credit status, and vacation preferences leave traces on machines and can be easily accessed when needed. The person under surveillance, consciously or unconsciously, provides the necessary data for surveillance by entering his/her insurance number, using his/her credit card, etc. Thus, surveillance is realized when access is provided to all transactions that people make by leaving electronic traces.[41] In the superpanopticon, the information collected about individuals is stored and analyzed in databases, and when necessary, it can be used for the strategic objectives of governmental authorities or companies.[32]

An additional conceptual framework that has gained salience, particularly in the context of information-communication technologies and contemporary social media tools, is the 'omnipticon.' The omnipticon introduces a novel paradigm of surveillance characterized by real-time interaction, where ubiquitous monitoring allows for the symmetrical observation of individuals, rendering both surveillance and being surveilled possible. In the digital age, people willingly take part in activities without external pressure, driven by entertainment or a desire for visibility. They continuously share information about themselves.[42] The pervasive use of social media platforms such as Instagram, Facebook, or X (Twitter) has significantly contributed to the phenomenon of the omnipticon, wherein individuals willingly share various aspects of their lives, hitherto considered private. This voluntary sharing stands out as a clear example of the omnipticon paradigm.

Discussion & Conclusion

A paramount concern associated with RFID microchips pertains to infringements upon privacy and the utilization of these technologies for surveillance objectives. When these implants are used, individuals become easily identifiable because the implanted microchips and their connected networks hold a significant amount of information, including sensitive data like health-related information. As articulated in the report by the European Group on Ethics in Science and New Technologies (EGE), these microchips, transforming individuals into interconnected entities, allowing their movements to be tracked, such as where they are and how much time they spend in a particular place.[43]

There also exists a potential vulnerability wherein the personal data stored in RFID microchips may be susceptible to unauthorized access.[12] Even though the FDA approved these microchips, it also acknowledged the potential risks to information security, alongside possible health risks associated with their utilization.[6] The FDA's approval of a technology not explicitly designated for therapeutic purposes, notwithstanding the identified risks, raises a separate and important discussion.

In the previous section, it was stated that Warren and Brandeis[21] defined privacy as "the right to be alone." Contemporary examinations, particularly in light of external technological applications such as smartphones and social media platforms, it's evident that just being alone doesn't automatically guarantee the protection of privacy. Similarly, when considering technologically embedded devices within the human body, mere physical isolation may not necessarily ensure the complete preservation of privacy.

Control-based definitions of privacy posit that individuals exert authority over who can perceive both their physical bodies and associated data, as well as the circumstances under which such access is permitted. Even if people willingly get microchips implanted, it's hard to guarantee they'll have control over who accesses the data stored on these microchips. Questions arise about who manages our health data in the microchip or its database, especially when doctors need to retrieve medical history in emergencies. Will the company creating the microchip or even our employers be able to see sensitive health data? And who's responsible if there are security issues? Currently, there are no clear answers to these questions.

Furthermore, just as the disclosure of a person's disease information would make him/her

vulnerable to his/her employer or insurance company, the disclosure of the fact that he/she carries an implant such as a pacemaker could pose a life-threatening risk. Therefore, privacy violations associated with RFID implants transcend conventional information technology breaches, evolving into significant concerns that need serious consideration, given their potential to endanger the dignity and lives of individuals. And, in the case of compulsory implantation, not only would we lose the ability to decide who can intervene in our bodies, but we would also surrender control of our personal data to external forces.

Contemporary media reports show a growing trend of using implants as a substitute for credit cards.[44] It's true that the risk of forgetting or losing a microchip implanted in the body is lower than losing traditional credit cards stored in physical wallets. However, when we consolidate all our identity information, including documents like driver's licenses, passports, and credit cards, onto a single microchip, our privacy becomes more vulnerable. This vulnerability arises from the potential for the illicit cloning of microchips, thereby facilitating the manipulation of all contained data.[5]

It appears highly probable that instances of privacy breaches will predominantly be driven by surveillance objectives. The implementation of microchips enables the potential retrieval of detailed information pertaining to individuals' works, home addresses, consumer preferences, social interactions, and the time spent in various places.[13] Such data accessibility facilitates companies in exploiting information without explicit individual consent, thereby precipitating a paradigm shift from subjects with agency to digital entities subjected to algorithmic manipulation.

RFID microchips will also emerge as an appealing technological device within capitalist systems. In alignment with Karl Marx's surveillance theory, which emphasizes the role of surveillance in boosting production within capitalist societies, these microchip implants could transform into potent surveillance tools in the hands of capitalist managers. This technology allows continuous monitoring of both factory workers and office professionals, eliminating the need for traditional methods of employee discipline. The constant awareness of being under surveillance encourages workers to discipline themselves and be more productive.[33] Although the use of microchips in companies today may seem voluntary, individuals might choose to adopt them reluctantly to avoid job loss, or they could be enticed by incentives like promotions or higher salaries for those who use the microchips.

At this point, a pertinent objection arises. Currently, individuals may already experience constant monitoring and surveillance by employers using company-issued mobile phones, vehicles, or computers, along with tracking entrance times through external access cards prevalent in many workplaces. However, the key difference with RFID microchips is their continuous integration into individuals' bodies, making them less easily deactivated compared to conventional devices like phones or computers. This means the control over surveillance isn't directly in the hands of the person being monitored. While external technologies enable surveillance up to a certain point, internal technologies allow continuous monitoring throughout every moment of our lives.

In the context of RFID microchips, the realization that surveillance goes beyond employees and employers to encompass every moment of life invokes thoughts of Foucault. While RFID microchips extend surveillance beyond Foucault's panopticon model, they can serve as highly functional tools for self-discipline. Within these microchips, which also store individuals' health data, bodies reduced to data will consistently monitor themselves to stay within the 'normal' range, showcasing the manifestation of power in every aspect of life.

Besides, the surveillance paradigm facilitated by RFID microchips aligns more closely with Mark Poster's concept of the superpanopticon rather than Foucault's panopticon. In Poster's concept, computer technologies enable the continuous and inconspicuous monitoring of a large number of people.[41] Through the electronic traces generated by implanted microchips beneath the skin, coupled with the personal data stored therein, a comprehensive set of information is collected and subjected to systematic analysis in databases. Subsequently, this aggregated data can be strategically utilized to serve the interests of those in authoritative positions.

Gary Marx also suggests that the way surveillance operates has changed due to new technologies.

The advent of novel technologies capable of penetrating deeply into individual realms enables categorical surveillance. In his 1985 article, Marx delineates the potential utilization of such surveillance technologies by governments targeting diverse demographics, including ethnic groups, religious minorities, or those deviating from societal majorities.[37] Contemporary advocacy for the implantation of microchips in migrants or guest workers[14, 45] align with Marx's predictions. Migrants, facing war and poverty in their home countries, may have no choice but to accept such practices when seeking refuge in another country for survival.

In addition to these, privacy advocates argue that the current voluntary nature of microchip implantation may evolve towards compulsion in the future. The normalization of practices such as implanting microchips in immigrants or individuals on parole from prisons, once accepted by society, it could be challenging to resist government efforts to monitor and control the entire population, justified by reasons of security or public health.[2] Examples of this potential include the contemplation of using RFID implants during the 2003 SARS outbreak in Singapore and the consideration of a mandate for microchip implantation in HIV/AIDS patients in Papua.[46] These instances show the tangible shift of mandatory microchip implantation from the realm of dystopian speculation into the active discourse of our daily conversations.

In conclusion, it seems that the use and discussion of RFID implants are becoming more common. Particularly in the contexts of conditions like Alzheimer's, dementia, or emergencies, it may be tempting to use these microchips for reasons such as identifying people and accessing their medical history. Moreover, ostensibly mundane, or presently considered "trivial" applications, such as the integration of microchips for operating printers[8] or facilitating financial transactions,[44] as reported in the media, may contribute to expediting societal acceptance of "implantable" technologies. However, although RFID implants offer certain conveniences, they do so at the expense of our privacy, freedom, and control over our lives. The concern is that we may only fully realize the extent of this sacrifice when it's already too late.

Conflict of Interest: None declared.

Ethical Approval Issue: No ethical approval was required for this study.

Funding Statement: This study received no specific funding.

References

1. Lockton V, Rosenberg RS. RFID: The next serious threat to privacy. Ethics and Information Technology 2005;7:221-231.
2. Gadzheva M. Getting chipped: To ban or not to ban. Information & Communications Technology Law 2007;16(3):217-231.
3. T.C. Resmi Gazete (Türkiye's Official Gazette). Kedi, Köpek ve Gelinciklerin Kimliklendirilmesi ve Kayıt Altına Alınmasına Dair Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik. Number: 31817, Ankara: Başbakanlık Basımevi 22.04.2022.
4. Özacar İU. 7 soruda evcil hayvanlara mikroçip uygulaması (7 questions on microchipping pets) TRT Haber 23.12.2022. Accessed 14.11.2023 https://www.trthaber.com/haber/turkiye/7-soruda-evcil-hayvanlara-mikrocip-uygulamasi-732986.html
5. Graveling R, Winski T, Dixon K, Cabrielli D, Desmullez M, Macdonald M. The Use of Chip Implants for Workers. European Parliament's Committee on Employment and Social Affairs EMPL, 2018. Accessed 28.12.2023 http://www.europarl.europa.eu/studies
6. FDA. Medical Devices; General Hospital and Personal Use Devices; Classification of Implantable Radiofrequency Transponder System for Patient Identification and Health Information, 2004. Accessed 29.12.2023 https://www.govinfo.gov/content/pkg/FR-2004-12-10/pdf/04-27077.pdf
7. Warwick K. Cyborg morals, cyborg values, cyborg ethics. Ethics and Information Technology 2003;5(3):131–137.
8. Cellan-Jones R. Office puts chips under staff's skin. BBC Technology, 2015. Accessed 12.12.2023 https://www.bbc.com/news/technology-31042477
9. Euronews. Dünyada mikroçip taşıyanların sayısı artıyor. 06.06.2018. Accessed 12.12.2023 http://tr.euronews.com/2018/06/06/dunyada-mikrocip-tas-yanlar-n-say-s-art-yor-iste-nedenleri
10. Gauttier S. 'I've got you under my skin'–The role of ethical consideration in the (non-) acceptance of insideables in the workplace. Technology in Society 2019;56:93-108.
11. Feder BJ, Zeller T. F.D.A. Approves Implantable Chip for Patient's Health Data. The New York Times, 2004. Accessed 14.12.2023 https://www.nytimes.com/2004/10/13/technology/fda-approves-implantable-chip-for-patients-health-data.html
12. Rotter P, Daskala B, Compano R. RFID implants: Opportunities and and challenges for identifying people. IEEE Technology and Society Magazine 2008;27(2):24-32.
13. Tucker Z, Boonthum-Denecke C. Security, privacy, and ethical concerns on human radio-frequency identification (RFID) implants: poster. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks 2019;322-323.
14. Foster KR, Jaeger J. Ethical implications of implantable radiofrequency identification (RFID) tags in humans. The American Journal of Bioethics 2008;8(8):44-48.
15. Altıparmak E. Sosyal Medya ile Değişen Mahremiyet Algısı. Master Thesis (in Turkish). İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü 2019;23.
16. Holvast J. History of privacy. In The history of information security. Elsevier Science BV 2007;737-769.
17. İlkılıç İ. Hasta Mahremiyetinin Antropolojik Belirleyicisi Olarak Utanma. In Hasta Mahremiyeti (Book in Turkish, ed. İlkılıç İ, Kucur C, Önder O). İstanbul: İSAR 2020;59-70.
18. Genesis 3:6-7, Bible, New International Version, https://www.bible.com
19. Quran, A'râf 7/22, https://quran.com
20. Quran, Nûr 24/27, https://quran.com
21. Warren S, Brandeis L. The right to privacy. The Harvard Law Review 1890;4:193-220.
22. Margulis ST. On the status and contribution of Westin's and Altman's theories of privacy. Journal of Social Issues 2003;59(2):411-429.
23. Altman I. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues 1977;33(3):66-84.
24. Moore AD. Privacy: its meaning and value. American Philosophical Quarterly 2003;40(3):215-227.
25. Fischer-Hübner S. Privacy and security at risk in the global information society. Information Communication & Society 1998;1(4):420-441.
26. Clarke R. Introduction to Dataveillance and Information Privacy, and Definitions of Terms, 1997. Accessed 23.12.2023 http://www.rogerclarke.com/DV/Intro.html#Aff
27. Finn RL, Wright D, Friedewald M. Seven types of privacy. In European Data Protection: Coming of Age. Springer, Dordrecht 2013;3-32.
28. Çakır M. İnternette Gösteri ve Gözetim (Book in Turkish) Ankara: Ütopya 2015.
29. Giddens A. Ulus, Devlet ve Şiddet. (Turkish Translation - Tr. C. Atay) İstanbul: Kaldeon Yayınları 2008; p.66, 237.
30. Akdağ G. 'Gözetim Toplumu' Teorilerinin Tarihsel ve Teorik Bir İncelemesi. Master Thesis (in Turkish). Aydın: Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, 2015;16.
31. Engels F. İngiltere'de İşçi Sınıfının Durumu. (Turkish Translation-Tr. O. Emre). İstanbul: Ayrıntı 2013;188.

32. Sönmez B. Gözetim Toplumunun Gümümüz Tüketim Dinamikleri Bağlamında Yeniden Yorumlanmasına İlişkin Bir İnceleme (Article in Turkish). Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi 2016;9(2):262-284.
33. Lyon D. The Electronic Eye: The Rise of Surveillance Society. MN: University of Minnesota Press 1994; p.25, 83-84.
34. Foucault, M. Discipline and Punish: The Birth of the Prison. Tr: A. Sheridan, New York: Vintage Books 1995;304-306.
35. Foucault M. Kliniğin Doğuşu: Tıbbi Algının Arkeolojisi. (Turkish Translation-Tr. Ş. Ünsaldı). Ankara: Epos Yayınları, 2002.
36. Foucault M. Cinselliğin Tarihi. (Turkish Translation-Tr. H. U. Tanrıöver). İstanbul: Ayrıntı 2016; p.100, 99-104.
37. Marx GT. The Threat of 1984-Style Techniques. The Futurist 1985;21-26.
38. Öztürk S. Filmlerle görünürlüğün dönüşümü: panoptikon, süperpanoptikon, sinoptikon (Article in Turkish). Gazi Üniversitesi İletişim Fakültesi İletişim Kuram ve Araştırma Dergisi 2013;36:132-151.
39. Okmeydan SB. Postmodern kültürde gözetim toplumunun dönüşümü: 'Panoptikon'dan 'sinoptikon've 'omniptikon'a (Article in Turkish). AJIT-e: Bilişim Teknolojileri Online Dergisi 2017;8(30):45-69.
40. Büyükgaga P. (2022). Dijital Gözetim ve Mahremiyetin Dönüşümü: 'The Circle' Örneği. Master Thesis (in Turkish). Ankara: Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü 2022;83.
41. Poster M. Critical Theory and Poststructuralism: In Search of a Context. NY: Cornell University Press 1989;122-3.
42. Bulur N. Gözetim Toplumu ve Yeni İletişim Teknolojileri: Z Kuşağı Üzerine Bir İnceleme. Master Thesis (in Turkish). İstanbul: Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, 2020;136.
43. European Group on Ethics in Science and New Technologies (EGE). Opinion on the ethical aspects of ICT implants in the human body. European Communities, Luxemburg, 2005.
44. Latham K. The microchip implants that let you pay with your hand. BBC News, 2022. Accessed 20.11.2023 https://www.bbc.com/news/business-61008730
45. Mack E. Presidential candidate suggests microchips for Syrian refugees. CNET, 2015. Accessed 14.11.2023 https://www.cnet.com/science/presidential-candidate-suggests-microchips-for-syrian-refugees
46. Michael MG, Michael K. Toward a state of überveillance [special section introduction]. IEEE Technology and Society Magazine 2010;29(2):9-16.