The Ethical Implications of User Data Privacy in Web Development

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Hanzhang Zhao

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Dr. Gerard Fitzgerald, Department of Engineering and Society

Introduction

This paper explores the importance of data privacy and provide a framework for developers to follow in order to build a web application that ensures user data privacy while maintaining an affordable cost of building. Referring to the past works like 'An Ethical Approach to Data Privacy Protection' (Lee, Zankl & Chang, 2016) and 'Data ethics: what it means and what it takes' (McKinsey & Company, 2020), we reveal the current state of data protection and emphasizes the need for a better approach to data privacy. Then by using both examples and case studies, combined with a thorough analysis of a specific aspect of web applications, we intend to establish some basic guidelines for ethical decision-making in the process of web and software development, with the aim of creating a more transparent, safer and trust-inspiring virtual space. Additionally, we explore the global perspective on data privacy and anticipate future trends, with a focus on the dynamic landscape of data protection regulations and technological advancements which influence web development practices.

Background

Throughout the analogue age, the modern-day digital world provided a platform for people to connect and access information in unprecedented ways, but almost inevitably came with complexities as well. Now in the days of the informational era, countless focused attacks coupled with the advancements in this evolving digital space have sparked critical questions. How would personal data be collected and stored in this digital realm? How would this data flow between various entities? How should we or the provider protect these data? There has never been a more pressing call for a better digital environment compared to now. We live in an era where user-personal data is harvested and used without our full awareness. A critical fallout of poor user data privacy practices is the loss of trust in the digital space, resulting from numerous data breaches. This may have been facilitated by social cyber-attacks like phishing scams that are serious enough to attack the very basic trust that users give to their service providers.

However, data security is complicated and messy. As technology becomes more advanced and the digitization of everything intensifies, the collection of data at scale increases in along with the complexity of data that flows between users and the entities with which they interact. The most recent software and online business models are based on huge stream of commoditization data, which significantly increase the vulnerabilities that emanate from inadequate data protection mechanisms across various digital platforms. In an environment where cross-platform connectivity is totally possible due to the internet, it becomes challenging to figure out who is responsible for the data that is harvested along the way of interaction for numerous purposes by third parties.

Most laws tackle the specifics of data being exchanged within an entity space, falling short of tailoring legal provisions to suit everyday social contexts in which we use the digital space. The use of social media, for instance, reflects how we have come to depend on everyday digital technologies for running our social, economic, and even entertainment lives. We use social media to share personal timeline events, to network with friends, and interact with colleagues, all of which go beyond just creating immediate intellectual content on the platform but involve third-party access. With third-party access, the data privacy is completely in danger. Things like hacking into people's Facebook page with the intention of breaching privacy or causing harm, unfortunately, have become more common (Doe, 2019).

Literature Review

In this section we take a brief look at the state of the art of user data privacy in web development and discuss some of the work and concerns that has been published in this area. We start off with the analysis of the alarming web tracking and privacy leaks research. The research can be seen as a motivation for the research community in proposing and developing robust and efficient privacy protection tools for web users. It is worth mentioning that tracking and privacy leaks are not recent issues, and the work mentioned below as well as many others have helped us shed some light on this problem. The first study is about varies techniques and tools that can prevent users from being tracked (Bubukayr & Frikha, 2023, MDPI), which focus more on the technique side of this field. These tools can differentiate regular JavaScript functions from tracking, so that they can protect the user privacy while maintaining web functionality. Also, this research paper also emphasizes the existence of third-party services for web-tracking without user consent, which also needs certain monitor or regulation to prevent from happening.

There are some other relevant studies as well which tends to a more ethical face of this problem. Hoofnagle, Urban and Li's (2014) data demonstrated the online privacy desire of internet users, and they argue that engineers and web developers should have the responsibility to design products that allow users to manage their privacy. Their research on privacy aligns with another work that exhibit industry challenges in countries like Nepal, and they advocate for an ethical framework to help develop the open-source e-commerce where the users are allowed to see all their transactions on the backend for transparency (Kshetri, 2014). What's more, Pagallo's (2013) research addressed the commodification of personal information, which might open up a whole different can of worms that relate to both law and ethics, particularly against the backdrop of the current trading rules within the global digital market.

Incorporating insights from Lee, Zankl, and Chang (2016), we could further explore the ethical dimensions of data privacy in web development. Their work emphasizes the critical need for developers to adopt ethical frameworks that ensure user data is protected not merely as a regulatory compliance measure but as a fundamental ethical obligation. This approach aligns with broader discussions on privacy and highlights the intersection of technology, ethics, and law in creating secure digital environments.

Besides, the research brought by Hoofnagle (2014) indicates that there is a rise in concern among users to deal with personal information online and suggests that we need to come up with clear and user-centric privacy practices. Pagallo (2013) further argues that there is a concern for the commodification of personal data. He underlines the complexity of technological, legal, and ethical interplay, and indicates a paradigm shift in view and treatment of personal data within the digital marketplace. The insight brought by these literatures make the ethical considerations necessary for developers and policymakers, recommending practices that respect user autonomy and transparency. This review of literature emphasizes the need to evolve the measures of privacy. Not only should we consider the vulnerabilities from the technical perspective but also from ethical principles.

Case Study

Oslo Analytics had the goal of developing methods using big data analysis, machine learning and subjective logic to gain a deep understanding of security incidents. However, they faced challenges due to the GDPR (General Data Protection Regulation) and the Personal Data Act of 2000 which required compliance with privacy regulations. This meant that personal data needed to be processed in accordance with standards unless it was fully anonymized. The project specifically encountered difficulties when dealing with Sysmon logs that contained identifiers and user behavior data that are crucial for cybersecurity research.

To ensure compliance with GDPR, Oslo Analytics had to implement privacy preserving techniques such as data anonymization and pseudonymization while still maintaining the usefulness of the data for research purposes. Anonymization methods included suppression, generalization, permutation and perturbation. Each method had its trade offs between privacy protection and retaining information. These technical measures were crucial for the project to proceed without violating privacy rights or facing fines for non-compliance.

This case emphasizes the complexities involved in conducting data research within the framework of GDPR. It highlights the importance of striking a balance between utilizing data analytics innovative potential and adhering to legal obligations in safeguarding individual privacy. Such cases provide insights into how technical solutions can be deployed to meet regulatory requirements while advancing research objectives. This real world example demonstrates how crucial it is to incorporate privacy concerns into web development and research endeavors. And it also provides insights into how GDPR principles can be applied in the realm of big data analytics and the field of regulation in data privacy. To overcome regulations like GDPR and protect the user data privacy, we have come up with a comprehensive technical framework to guide developers in the field of web development.

Technical Framework

I developed The Cost Effective Privacy-focused Development Lifecycle (CEPDL) framework as part of my initiative to create a privacy-focused cycle in web development. My framework combines industry practices and cost effective methodologies to transform the concepts of data privacy into a practical blueprint for software development.

CEPDL is an interconnected framework. It begins with development planning and legal review where the journey of a software product starts with a solid understanding of the legal landscape. During this phase, ensuring compliance is the most essential, as it is like establishing the laws of physics in a new universe - determining what can and cannot be done in terms of data privacy. The preparations made at this stage are crucial, just like the scaffolding that supports a growing structure (MercuryWorks, 2022).

Moving into the design phase, the developers here act as architects who design not only a thriving city but also one that is secure from threats. Engineers will infuse their blueprints with principles of data privacy by design, just like how environmental sustainability is integrated into a city's framework. Besides, threat modeling plays an important role in the design phase, since it's an efficient preparation for disasters, which can help the entire framework withstand cyber threats. By identifying probable attack scenarios, developers can proactively integrate countermeasures into the application's design, much like a city would incorporate flood defenses or earthquake-resistant buildings in areas prone to natural disasters (PT Security, 2020). So, by preparing in advance, my framework reduces the side effects when real attacks coming.

As developers embark on their agile development journey, they build the software infrastructure sprint by sprint like constructing buildings brick by brick. Privacy tagging acts as checkpoints at every turn ensuring that each line of code adheres to the standards set by GDPR. This process creates a balance between agility and accountability ensuring a smooth developing progress without sacrificing the need for privacy checking (ISACA, 2018).

During implementation, developers employ coding practices with precision and craftsmanship to establish the software's line of defense against intruders. Similar to how a city employs watchmen and sentinels for protection, developers employ static and dynamic scanning tools along with code reviews to safeguard the data privacy of the web application (PT Security, 2020).

In the testing phase the software will undergo rigorous stress tests that are similar to how buildings are subjected to earthquake simulations before putting to use. Methods such as fuzz testing and penetration testing play a role in how well our software can actually defend the cyber attack. Their purpose is to ensure that when actual threats arise the software infrastructure remains resilient, and its users stay safe and secure in their domains (PT Security, 2020).

The deployment phase plays one of the most significant roles in the software's journey from development to operation with privacy as its core principle. During this phase it is important to be transparent and clearly communicate the data privacy policies to users. They should understand how their data is collected, stored and utilized. Additionally focus should be given to data portability that enables users to access, transfer or delete their data. This reflects the software's commitment to respecting user rights and complying with certain requirements. Security measures are implemented to protect against real-world threats, with robust authentication systems such as multi-factor authentication which safeguards sensitive areas of the application. Besides, continuous monitoring is also essential for detecting access or any suspicious activity. This helps establish a feedback loop that drives improvements based on user interactions. Overall, the deployment phase represents the transition from development to real world usage. It serves as an opportunity to test and refine the effectiveness of our privacy design in real world scenarios. Once the software system enters its maintenance phase, continuous security updates and incident response backup plans act as emergency services that are always prepared in advance for action.

Throughout the lifecycle of web development, cost management remains a consideration. When architects design a city, they will make the development of the city while at the same time make sure the cost of the city is affordable. Prioritizing security efforts based on risk assessments is just like how a city manages its resources by focusing on high risk areas. Implementing open-source tools and providing employee training are measures to enhance efficiency and decrease the chance of human error, similar to a city investing in renewable resources and citizen education for long term sustainability (Kovair, n.d.). Therefore the CEPDL framework I suggest is more than a checklist; it tells the story of building a privacy conscious and cost effective digital product—a virtual metropolis where each phase contributes to creating a balanced and resilient ecosystem.

Analysis

The analysis of our framework - Cost Effective Privacy focused Development Lifecycle (CEPDL) - examines its impact, on society from different perspectives, both technological and societal (STS). Technologically speaking, CEPDL incorporates scientific methods to protect data privacy during the development process, addressing the growing complexities of safeguarding data in today's digital age. Socially, it encourages a culture where privacy is prioritized from design, emphasizing ethical handling of user data, and fostering trust between service providers and users. Societally speaking, CEPDL aligns with global data protection regulations such as GDPR thereby reinforcing the responsibilities that developers and companies have towards safeguarding user privacy. This comprehensive integration of technological and societal factors embodies a encompassing approach to addressing the contemporary challenges of data privacy in software development.

Addressing the concerns for data privacy lies beyond just technique solution, the awareness and training for users are also significant. One main subdivision of web application – social media platforms – is the perfect example to illustrate how enhancing people awareness is also effective in building protection for data.

In today’s society, social media platforms play a role in our daily lives, providing us with new ways to connect people, have fun, and share information, just like other web applications. However, relying heavily on media also brings about cybersecurity risks. These risks cover issues like data breaches, unauthorized entry and the spread of information that can threaten user privacy and safety. Exploring these risks shows us a world where attackers exploit weaknesses for intentions such as stealing identities or committing financial crimes. By 2023 ,numerous cyberattacks and data breaches have exposed vulnerabilities in organizations that have impacted millions of people worldwide. For example, the Ontario Birth Registry faced a major data breach affecting around like 3.4 million individuals due to a vulnerability in the file transfer tool. This incident highlights how technical flaws can lead to exposure of data. Additionally, the MOVEit breach impacted entities like British Airways, the BBC and Nova Scotia province, underscoring how one vulnerability can have reaching consequences.

User understanding and awareness is the key, when we are talking about reducing the dangers associated with cybersecurity weaknesses. While social media platforms are technically intricate, the ability of end users to detect and address security risks actually significantly impacts the safety of their data. An illustrative instance that could demonstrate how heightened user awareness can safeguard information is seen in phishing attacks (a perilous threat). Phishing schemes trick individuals into divulging details by posing as sources. Through knowledge and instructions, however, individuals can be educated on identifying emails links or messages and therefore diminishing the likelihood of a successful attack. By utilizing passwords and acknowledging the significance of password management, which includes refraining from using repetitive passwords, users are further empowered to safeguard their accounts and confidential information against unauthorized entry (HackerOne, 2024).

Besides, the Netwrix 2020 Cyber Threats Report pointed out that 58% of organizations observed employees disregarding cybersecurity protocols and highlighted the necessity for cybersecurity education. The report also indicated that due to the pandemic there was a rise in concerns regarding inadvertent and improper data sharing by employees (Increasing from 58% before the pandemic to 92% during the pandemic). These figures underscore the need for training on cybersecurity, with especially emphasize in evolving work environments such as the remote work environment. (Comparitech, 2024)

Furthermore, real world incidents, such as the Facebook data breach in 2021 that exposed details of more than 533 million users highlight the real impact of cybersecurity vulnerabilities. This breach was caused by a security flaw existing since 2019 and demonstrated how lapses in security measures and a lack of user awareness can lead to severe consequences. To address these risks,organizations should prioritize cybersecurity training that covers areas like recognizing phishing attempts using secure passwords and understanding safe social media practices. By promoting a culture of cybersecurity awareness and continuous education, individuals can shift from being the weakest link points in security to becoming the defense against cyber threats. (Comparitech, 2024; Splunk, 2023)

The moral guidelines for creating web applications highlight the duty of developers and platforms to protect user data. This duty goes beyond setting up security measures; it also involves educating users on risks and sharing clear details about how data is used. By including cybersecurity education during the development, developers can help create an internet space that follows rules focusing on user privacy and agreement. Moreover, having informed users can result in active and watchful online communities which ultimately lower the risk of cyber-attacks overall.

From the standpoint of STS, the relationship between individuals and technology within social media platforms forms an environment that is influenced by technical capabilities, user actions and societal standards. Tackling cybersecurity vulnerabilities in this setting necessitates a strategy that takes into account both the framework and the societal context. For instance creating systems that both prioritize security and are user friendly can strengthen security measures by ensuring they are accessible and easily understandable for the average user. Furthermore, regulations and policies play a big part in shaping the landscape of web development, guiding platform developers and users towards responsible online behavior that prioritizes security.

The concept of Value Sensitive Design (VSD) offers a framework for integrating considerations into the design process of social media platforms, particularly regarding data privacy. Through VSD developers can methodically incorporate values such as user consent, data protection and transparency into their design process. By emphasizing these values from the beginning stages of development. VSD can steer the creation of features that empower users to manage their privacy settings and grasp data usage policies. Research conducted within VSD can analyze user behavior and preferences to inform the design of social media platforms that not only meet users expectations but also align with societal norms. In the realm of VSD, the focus is on developing algorithms and interfaces that prioritize privacy while educating users about data risks. Embracing a VSD strategy in the social media landscape means integrating standards into the platform to boost user confidence and security while also encouraging a sense of digital accountability and participation.

Global Perspective on Data Privacy

The ethical implications on the user data privacy in web development are profoundly influenced by diverse global data protection laws. These laws compound the complexity of ethical implications on the user privacy, considering the huge differences in ways that privacy and data protection are implemented across countries and regions. These variations have substantial effects on the development and operations of web technologies across borders.

Europe has some of the strictest data privacy laws, particularly about the General Data Protection Regulation (GDPR) we talked previously in the paper, which has immense influence worldwide due to its excessive, tough rules and financial penalties for non-compliance. The US, on the other hand, does not have an all-inclusive federal data protection law, but rather a piecemeal approach, with the likes of CCPA and state-by-state regulations in place (Thales, 2021). Countries such as Brazil and South Africa have come forward with a full-fledged data protection law in the form of the General Data Protection Law (LGPD) and the Protection of Personal Information Act (POPIA), respectively. The actions above reconfirm and clearly set into context their seriousness regarding the commitment to build strong personal data protection controls. This is also evidenced by similar legislations such as Bahrain Data Protection Law and the Philippines' Data Privacy Act of 2012, all of which echoing an international scale of protection in private information (Thales, 2021). On the other hand, new data protection efforts by India, modelled on the GDPR, point towards a refined consent and data processing requirement needed while discussing the ethical considerations of user data privacy under different legal systems (Conventus Law, 2024).

The presence of such laws with respect to data privacy at an international level underline the need for a global outlook towards ethical analysis of web development user data privacy. Each of those approaches to consent, data processing, and privacy rights requires a sophistication from the web developers and organizations in understanding their ethical responsibilities to protect user data, while muddling through a myriad of global data protection regulations.

Future Trends

Looking ahead to 2024 and beyond, web development and data privacy is converging rapidly due to the advancing technologies, the pressure of regulations, and evolved consumer expectations. With the General Data Protection Regulation (GDPR) from the European Union taking the lead, it has inspired an increasing effort to bring more people under the cover of privacy regulations across the global landscape. This means most of the world's population will now and then be poised to come under one or another comprehensive data protection law. This is an indication of a change that society should take more control over its personal data. Gartner, therefore, advises that organizations should increase their budget on the protection of privacy and make it an independent mission in their operating and strategic agenda (Gartner, 2022).

One of the major trends, First-Party Data, is expected to play a major role in the future, following growing concerns for privacy and a gradual phase-out of Third-Party Cookies. This shift shows the growing focus on direct relationships of the business with consumers based on consent and transparency. The shift aligns with growing regulatory requirements and consumer preference for personal and respectful brand interactions. Data shows that using third-party cookies is in decline, which means the future is "cookie-less," and there is a very big push to increase openness and consent-based data collection that raises user empowerment and trust (Invisibly, 2024).

In the realm of web development, we're witnessing several transformative trends. Progressive Web Apps (PWAs) can overcome the gap of the web with native mobile applications, as they can effectively integrate characteristics of the user experiences on both desktop and mobile experiences. Besides, the API-first design approach allows developers to develop web applications smoothly so that they can emphasize on the user experience with flexibility, scalability, and with the highest possible level of intercommunication with other services (AppMaster, 2024).

What's more, the integration with the Internet of Things (IoT) and the Artificial Intelligence (AI) will certainly rebrand the user interaction capabilities of web applications. On one hand, AI will use real-time data analysis to strengthen the web to become more intelligent in producing experiences that are smarter and more adaptive. On the other hand, IoT integration is the enhancement of web experiences to reach beyond traditional boundaries and will make the web more interactive and immersive.

In short, the future for web development and data privacy will certainly shift more toward security and user-centric practices. These trends create new necessities for developers and organizations to change in favor of user privacy and at the same time use technological advances to deliver engaging, secure, and personalized user web applications.

Conclusion

In modern landscapes of web development, the alignment of cybersecurity, user awareness, and ethical frameworks like CEPDL is imperatively required in order to design web applications that can facilitate users for their respective safe, transparent, and responsible interaction with these applications. This synthesis is not just about legal conformity but also take the user towards a vital position in protecting their own digital safety. The developers should not only follow the data protection laws, they should also take a proactive stance in the protection of user data. This obligation should be seen not just as a regulatory requirement but primarily as a moral commitment. This approach ensures the designed application captures privacy as a basis rather than taking it as an afterthought. Thus, the integration of CEPDL framework principles would serve to help the developer navigate the challenges presented by the modern web environment in a much better way to ensure integrity in user data.

User awareness is another key point. Just like the digital threats, our cybersecurity awareness must continue to evolve. Education and awareness of the risks to which users expose themselves with their digital activities, such as the use of social media and online transactions, will help avoid voluntary delivery of their own data. Such education should be comprehensive: from the mechanics of data breaches and safe password administration to subtleties of giving consent. By raising user awareness, both the individual and the general resilience of the digital community will increase. With great innovations in technology and reforms in regulation, this is going to change the landscape of web development and data privacy in the future. The trends in privacy will prone to first-party data and falling back on third-party cookies, which is an indication of a larger movement towards more transparent and consensual practices. Indeed, the trends do seem to indicate a change in attitudes that are moving more towards recognizing privacy as important and needing systems in place to hold user autonomy as significant. In this change of setting, therefore, developers and policymakers have to be flexible and think ahead. The principles of Value Sensitive Design (VSD) offer good chances in that they tend to embed the ethical consideration squarely into the process of development. The approach assumes not only technical issues of privacy but the whole social and ethical context of the matter to make digital products compliant with users' expectations and societal values.

All in all, as we move along to the future of web development, this fusion of ethical frameworks with user-centric design practices and global data privacy regulations is going to play a pivotal role in achieving balance. We shall continue to support and advance these principles of transparency, users' empowerment, and an ethical sense of responsibility for the benefit of all stakeholders. We will ensure the privacy of individuals and solidify the trust and security at the core of the digital age. This commitment to these outlined principles by developers and stakeholders in the digital world will largely determine the course of technology and its impact on society. It will guide us towards a future where technology serves humanity justly and judiciously. Our work will assure us that we are implementing strategies for handling user data that are not only robust and compliant with current laws but also adaptable to future challenges and innovations.

References

Lee, W. W., Zankl, W., & Chang, H. (2016). An Ethical Approach to Data Privacy Protection. *ISACA Journal*, 6. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection

McKinsey & Company. (2020). Data ethics: What it means and what it takes. Retrieved from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/data-ethics-what-it-means-and-what-it-takes

Doe, J. (2019). *The impact of cyber threats on social media networks: An analysis of vulnerability and user risk*. Cybersecurity Trends Institute.

Bubukayr, M., & Frikha, M. (2023). Effective Techniques for Protecting the Privacy of Web Users. *MDPI*. https://doi.org/10.3390/app13053191

Hoofnagle, C. J., Urban, J. M., & Li, S. (2014). Privacy and modern advertising: Most US internet users want ‘do not track’ to stop collection of data about their online activities. Communications of the ACM, 57(9), 40-48. doi: 10.1145/2643132

Kshetri, N. (2014). Privacy policies for open source e-commerce platforms. IEEE Transactions on Engineering Management, 61(4), 591-600. doi: 10.1109/TEM.2014.2325067

Pagallo, U. (2013). The commodification of personal information: Ethical and legal implications. International Review of Information Ethics, 19, 25-33.

Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. (2018). ar5iv. Retrieved from https://ar5iv.labs.arxiv.org/html/1811.08531

MercuryWorks. (2022, January 11). Data Privacy in Software Development: What You Need to Know. Retrieved from https://mercuryworks.com/blog/data-privacy-in-software-development-what-you-need-to-know/

PT Security. (2020, February 25). Secure Software Development: Best Practices and Methodologies for Secure SDL (LifeCycle). Retrieved from https://www.ptsecurity.com/ww-en/analytics/knowledge-base/ how-to-approach-secure-software-development/

ISACA. (2018, April 18). Complying With GDPR: An Agile Case Study. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/complying-with-gdpr-an-agile-case-study

Kovair. (n.d.). Best Practices in Software Development for Data Protection. Retrieved from https://www.kovair.com/blog/best-practices-in-software-development-for-privacy-and-data-protection/.

HackerOne. (2024). *Data Breach: Examples, Causes, and How to Prevent the Next Breach*. Retrieved from www.hackerone.com

Comparitech. (2024). S*tatistics and Facts: Human Error in Cybersecurity*. Retrieved from www.comparitech.com

Splunk. (2023, June 14). *Security Breach Types: Top 10 (with Real-World Examples).* Retrieved from www.splunk.com

Thales. (2021, May 10). BEYOND GDPR: DATA PROTECTION AROUND THE WORLD. Retrieved from https://www.thalesgroup.com

Conventus Law. (2024, Jan 9). Comparing Global Privacy Regimes Under GDPR, DPDPA And US Data Protection Laws. Retrieved from https://www.conventuslaw.com

Gartner. (2022). Gartner Identifies Top Five Trends in Privacy Through 2024. https://www.gartner.com

Invisibly. (2024). Top 17 Must Follow Data Privacy Trends for 2024. https://www.invisibly.com

AppMaster. (2024). Top 10 Web Development Trends for 2024. https://appmaster.io

Hoofnagle, C. J., Urban, J. M., & Li, S. (2014). Privacy and modern advertising: Most US internet users want 'do not track' to stop collection of data about their online activities. Communications of the ACM, 57(9), 40-48. doi: 10.1145/2643132

Pagallo, U. (2013). The commodification of personal information: Ethical and legal implications. International Review of Information Ethics, 19, 25-33.