The Information Privacy Contradiction

Interest-Based Posture of Compliance and Violation

From every conceivable perspective, data are tactical, operational and strategic assets.[1] Striking the right balance between the societal need for data and the right to information privacy has been a challenge for individuals, organizations and nations. There has been a tendency to rely on ethics and expect entities to do what is right with the personal and enterprise data they amass. The problem is that reliance on ethics is not enough. The effectiveness of information privacy compliance depends in part on the capacity of all entities to reflect on the challenge constantly, substantively and continuously and be willing to allow societal interests to mostly outweigh other interests. Unfortunately, no matter how much individuals, groups, organizations or nations embrace that philosophy, the dialectic of self-interest makes perfect compliance virtually impossible. There is an information privacy contradiction, with compliance and violation like two sides of a coin—tendencies toward compliance on one side and violation on the other side. Every entity or actor has both information privacy compliance and violation tendencies.

The issue then becomes choosing an information privacy side, either mainly exploiting it, protecting it or perhaps falling somewhere in between. Most entities, regardless of culture or level of sociopolitical or socioeconomic standing, tend to be on either side at different times, depending on their interests and motivations. Motives that change with time and circumstances often determine the winning side of the information privacy coin.

Although tolerance of information privacy exposure differs, based on time and circumstances, individuals, groups, institutions and organizations generally prefer the right to be left digitally alone.

Yet individuals, organizations, institutions, businesses, government agencies and nations ferociously exploit others' personal data or enterprise data while doing everything to preserve their own—hence the information privacy contradiction.

There is an information privacy contradiction, with compliance and violation like two sides of a coin—tendencies toward compliance on one side and violation on the other side.

If there were no contradiction, information privacy guardians and offenders would be more easily identified, tracked, rewarded or punished, and

PATRICK I. OFFOR | PH.D.

Is an associate faculty member at the City University of Seattle (Washington, USA). He has published many peer-reviewed articles on information systems security and information privacy. He is also a US Department of the Army civilian.

Applying and maintaining information privacy rights in the context of current societal constructs is difficult because the world has shifted from being siloed or segregated to being integrated, interconnected and interdependent.

information privacy actors would be classified simply as exploiters or guardians without much complexity of analysis. However—and relative to what is evident in information security, cybersecurity and other disciplines—information privacy actors who perpetrate malicious or nonmalicious intrusions at one point may at other times be guardians, defenders, promoters or advocates of information privacy. For example, cybersecurity and information security administrators with network and physical access battle the demon of introducing network intrusion when provoked and guarding their systems against both nonmalicious leaks and malicious attacks, despite provocations, depending on changing times and circumstances.

For practitioners and researchers, the natural next step is implicitly or explicitly identifying and discussing the information privacy contradiction. However, to sufficiently evaluate and articulate the essence of this contradiction, one must assess at the very least the adequacy of current information policies, laws and regulations around the globe at the individual, organizational and national levels. Regulatory attempts at information privacy compliance will always be unsatisfactory without an understanding of the contradictions of information privacy realities and how to embed them into policy and regulatory enactment processes and enforcements, including understanding some key issues:

- Why people will do everything to preserve their own data but have limited or no reverence for other people's data
- Why managers and responsible agents preserve their organizations' trade secrets, intellectual properties and technical know-how but readily trade personal and enterprise data of others for profit
- Why there are comprehensive to semicomprehensive policies, laws and regulations on information privacy in some countries and not in others

Information Privacy

Information privacy is concerned with enterprise and individual rights to their data and information, and principles and practices governing data management by others. Understanding the right to privacy and the right to control personal data and information in theory and in practice is the cornerstone of information privacy conceptualization and construction. However, applying and maintaining information privacy rights in the context of current societal constructs is difficult because the world has shifted from being siloed or segregated to being integrated, interconnected and interdependent—socioeconomically and sociopolitically. Access to information and the need for information privacy arose together as technology granted access to other peoples' information, whether authorized or not, even from distant locations. In today's connected world, the omnipresence of Internet-enabled devices that generate an insatiable appetite for socioeconomic, sociopolitical and technological advancement is not a bad thing in itself. However, it has led to information privacy becoming crucial to control access to sensitive personal data, protect health information, guard intellectual property and establish boundaries for the use of surveillance, legal, religious identification and sexual orientation information.[2]

Contradiction

The law of noncontradiction is that "It is impossible for the same thing to belong and not to belong at the same time to the same thing and in the same respect."[3] Based on that perspective, the argument of information privacy contradiction may seem to be a nonissue because reality cannot contradict itself. However, when evaluating information privacy reality based on time and circumstances, contradictory positions and decisions become apparent. When discussing contradictions in information privacy, some of the questions that arise are whether a contradiction exists, why it exists, how it exists, what impacts it has and the practical and theoretical implications therein, if any.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Existence of Contradiction in Information Privacy

Information privacy reality comprises the practical feelings, thoughts, conditions and occurrences relating to collecting, using, storing, controlling or managing private data or information at an individual, group, enterprise, institutional or national level. There are many instances of information privacy realities in one information privacy event, including:

- Being the subject of an information privacy gathering
- Being the recipient of information privacy data
- The perception of concern or the absence of concern about the disclosure of data or information
- The awareness, feeling or thought of having control over personal or enterprise data or information or of not having such control
- The awareness, feeling or thought that disclosing personal or enterprise data or information is more beneficial than avoiding disclosure
- The belief that revealing data or information is riskier than avoiding revelation
- An understanding of the values of information privacy
- Being neither a data or information privacy subject nor a recipient, but understanding the associated values, benefits and risk

Although contradiction does not exist in reality because reality does not contradict itself,[4] there are many cases in which assessments of reality are contradictory. If a group of people on the street are asked where they stand on information privacy, some will consistently favor it while others will be against it or remain in the middle. For example, in countries with multiple major political parties, there are ever-present changes in political viewpoints and affiliations among the populace. As another example, in questionnaires, the lack of response to an optional two-item selection will change over time. The point is that two or more people, groups, organizations or nations are likely to see reality differently based on their interests, and their assessments of the same reality will likely change over time and under different circumstances. Although the core information privacy principles of data privacy and control of information are acknowledged, understood and accepted, attitudes toward enforcement fluctuate among effectuation, nonenforcement and indifference. Thus, the contradiction in evaluating the reality of information privacy as entities is a constant, just as a change is itself a constant. **Figure 1** is a presentation of the components of information privacy reality and its coding.

Figure 2 illustrates the information privacy assessment and positioning or decision and contradiction realities using the underlying principles in the union and intersection of sets scheme.[5] A Venn diagram can be used to express the union and intersection scheme fundamentals. **Figure 2** accounts for all mutual and exhaustive possibilities of information privacy actors.

Individuals (D1), groups (G1) and organizations (O1) are subjects of information privacy gathering at a time (Time #1) of the information privacy reality (PR). D2, G2 and O2 are the recipients of information privacy. Conversely, at PR Time #2, D1, G1 and O1

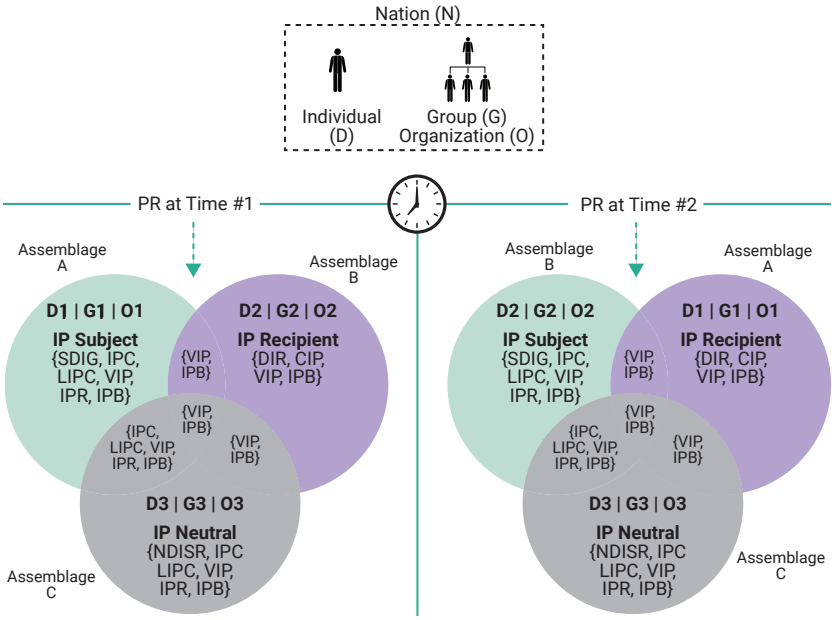
FIGURE 1

Components of Information Privacy Reality

Information Privacy Reality	Reality Coding	Subject	Recipient	Neutral
Control of information—Personal or enterprise	CIP		X	
Data/Information recipient	DIR		X	
Information privacy benefits	IPB	X	X	X
Information privacy concerns	IPC	X		X
Information privacy risk	IPR	X		X
Lack of information privacy control	LIPC	X		X
Neither a data/information subject nor recipient	NDISR			X
Subject of data/information gathering	SDIG	X		
Value of information privacy	VIP	X	X	X

FIGURE 2

Information Privacy Interest Contradiction Model



become the recipients of information privacy data, whereas D2, G2 and O2 become the subjects of information privacy gathering. D3, G3, and O3 are the neutral parties at PR Time #1 and Time #2 and do not have a play at the time horizon under discussion. However, they could easily be information privacy subjects or recipients based on changes in their interests or in other instances of time within the continuum of time. Note that all the actors in any of these assemblages could come from one nation (N) or from multiple nations. The applicability of the conceptual illustration in **figure 2** could also be for a nation, institution or other entity.

In PR Time #1, the information privacy subject would be apprehensive and concerned about the collection, use and storage of their personal, group or enterprise data because they lack the appropriate control over the data and the risk therein, even though they understand the value and benefits of the data to themself and others. However, when the subjects becomes the information privacy recipients in PR Time #2, their focus would be on the added value and benefits of the data to themselves, the group or the organization because their interests and motivation have changed. The change in position could also be because a person or organization needs to have the ability to control the data as a data recipient.

The intersections in **figure 2**, also detailed in **figure 3**, support several observations.

Information Privacy Reality Timeline #1

The information privacy reality shared by Assemblage A (subject) and B (recipient) comprises the values and benefits of information privacy (value of information privacy [VIP] and information privacy benefits [IPB]).

Assemblage B controls the data upon receipt because it is the designated recipient of the data in this case. Consequently, Assemblage B has limited to no concerns for the data or the potential risk therein, even though it is aware of the potential cost of data disclosures to the data subjects.

Although Assemblage C (neutral) shares information privacy concerns, due to the lack of personal data control and the value, risk and benefits of information disclosure with Assemblage A, it remains neutral because it is neither a subject of information

FIGURE 3

Information Privacy Reality Intersections Timeline

PR Timeline	Assemblage		Intersection		Intersection Set Detail				
Time #1	A	B		A ∩ B	VIP	IPB			
	A	C		A ∩ C	VIP	IPB	IPC	LIPC	IPR
	B	C		B ∩ C	VIP	IPB			
	A	B	C	A ∩ B ∩ C	VIP	IPB			
Time #2	B	A		B ∩ A	VIP	IPB			
	B	C		B ∩ C	VIP	IPB	IPC	LIPC	IPR
	A	C		A ∩ C	VIP	IPB			
	B	A	C	B ∩ A ∩ C	VIP	IPB			

gathering nor a recipient of it. Information privacy neutrality is a state or condition in which one is neither a subject nor a collector of another's personal, enterprise or national data. For example, an entity is information privacy neutral if it is neither an information privacy subject nor a recipient in an information privacy event.

Assemblage A realities include being the subject of data or information gathering, having an information privacy concern, having a lack of information privacy control, understanding the values of information privacy, being aware of information privacy risk, and having cognizance of information privacy benefits.

The only reality common to all assemblages, regardless of the information privacy reality timeline, is understanding the values and benefits of information privacy (VIP and IPB). This is partly because even though Assemblage B is aware of the associated information privacy risk, having been the subject of information privacy at one time, it gives it little consideration so as not to impede its objective as an information privacy recipient.

Information Privacy Reality Timeline #2

Although there is a swapping of the assemblages' positioning in reality timeline #2, Assemblages B (subject) and A (recipient), still share the same information privacy values and benefits (VIP and IPB). In other words, a person, organization or group does not lose its information privacy values or benefits perspective even when operating as an information privacy subject or recipient.

Personal, enterprise, institutional or national concern for data or information privacy is manifested and heightened when one is the subject of information privacy and obscured and minimized when one is the recipient of information privacy. This observation is no different from what happens in intelligence communities around the world (i.e., China's Ministry of State Security, France's Directorate-General for External Security, Germany's Bundesnachrichtendienst, Israel's Mossad, the UK Secret Intelligence Service, and the US Central Intelligence Agency [CIA]).[6] If nothing else, the common thread among these intelligence agencies is that they simultaneously embody this contradiction. The agencies are renowned for defending or protecting their information while exploiting other agencies' and personnel's information, meaning that they epitomize both information privacy subjects and recipients at any given time.

Information privacy reality timelines #1, #2 and #n (any number) for an individual, group, organization, institution or nation could run intermittently or concurrently.

Rationale for Information Privacy Contradiction

The unity of opposites exists in everything. The outcome of the unity of opposites is the catalyst and driver of information privacy advancements. Information privacy contradiction is rooted in the suggestion that the absoluteness or universality of contradiction is present in all developments and that in each development lifecycle, the dialectic movement of opposites exists.[7] Further, it is rooted in the notion that actions depend on the outcome of the dialectic dogma of self-interest or self-centeredness and that self-interests change over time based on prevailing circumstances.

It is useful to address the unity of opposites as it relates to materialist dialectics, self-interest and their convergence to answer the question of why the information privacy contradiction exists and will continue to exist regardless of the prevailing laws, directives, policies and regulations, including:

- **The Unity of Opposites**—The unity of opposites poses a struggle in many individuals' day-to-day activities and everyday lives. For example, within one individual, there are struggles between liking and hating things or people. There are struggles between strengths and weaknesses in capabilities, between truths and lies, between integrity and dishonesty. There are struggles between motivations and lack thereof, and between support for things, activities and people and the lack thereof. Underlying the struggles in each information privacy actor is the fact that opposites exist. An actor's privacy behavior in an information privacy event largely depends on the dominance of an opposite driven by the actor's information privacy reality postures in time and circumstance, which means that an information privacy actor's behavior would naturally differ depending on whether the individual was a subject of information privacy gathering, a recipient or was in a neutral state.
- **Materialist Dialectics**—Materialist dialectics hold that development arises from the contradictions

What a person views as important at a time has a bearing on whether to protect or exploit private or enterprise data under given circumstances.

within a thing. It suggests that external causes are the condition of change, while internal causes are the basis of change. Hence, external causes become operative through internal causes.[8] For example, an egg changes into a chicken at a suitable temperature.[9] The temperature change is quantitative and external, and it provides the condition for the egg to become a chicken. However, the basis for the change of the egg to a chicken is qualitative and internal. With a quantitative change, an object does not lose its form even when its quantity, degree or measurement changes. In contrast, with a qualitative change, an object or thing would steadily transform amid the change.[10] Therefore, in the context of information privacy, individuals and organizations, among other entities, are dialectically, externally and quantitatively motivated at intervals by their interest in violating other peoples' privacy while they are simultaneously internally and qualitatively motivated to steady their information privacy defenses against violators. The interests can be any number of things, such as profit or process improvement, or they can be innovation-driven. This dialectics of opposites in information privacy is not confined to the discipline alone. The push and pull—that is, the drive for unity and the struggle of opposites—underlies all human developments, including information privacy policy development, education, training, awareness and compliance.

- **Self-Interest**—The notion that human beings are primarily motivated by self-interest is shared widely.[11] Self-interest is what an individual views as important at any given time and does not necessarily have to be only about the self. In other words, self-interest could be something meaningful to the self or what an individual considers important about other people, events, organizations, entities or personally essential beliefs.[12] The concept of thought relating to individual actions is supported in literature because, naturally, humans consciously or unconsciously think about something before doing it, whether the thought is rational or not. This is because for every action taken, whether it is within the context of an individual or an entity, there is thought, feeling, physiology and an act.[13, 14] Therefore, in the information privacy arena, what a person views as important at a time has a bearing on whether to protect or exploit private or enterprise data under given circumstances.

In the rope-pulling sport called tug-of-war, at least two people or two groups of contestants are at opposite sides of a rope during the game, each pulling hard in an effort to drag their opponent toward the center and across a line to score a win. However, in contrast to the information privacy contradiction, only one contestant mentally pulls the rope away from the center (neutral) toward the right (protection) or left (exploitation). The contestant's self-interest and information privacy realities at the given time and circumstances determine whether the information privacy actor protects or exploits personal or enterprise data or takes an indifferent posture.

Information Privacy Contradiction Cases

Consider the following cases in which organizations played an active role in exploiting users' data, even without the admission of guilt during the subsequent settlements.

Case 1—Google

Google has extensive measures to protect users' information. Its privacy policy and terms explain the types of data Google collects, how those data are stored and used, and the attempts Google makes to keep private and enterprise data safe, including providing the Google Incognito browser for private browsing on the Internet.[15]

The core privacy principle espoused by Google is to respect users' privacy, to provide clarity about the type of data it collect and how those data are used; to promise to not sell users' data; to provide control mechanisms that allow users to exercise some control over their information by using on/off switches; to provide users with a mechanism to review, move or delete their data; and to constantly invest in capabilities that advance information systems solutions.

Data Exploitation

Two children sued Google in April 2020 for exploiting their data. The allegation was that Google used legitimate services, Chromebook, and free access to G Suite for Education applications provided to schools in San Jose, California, USA, to collect unauthorized biometrics information from the pupils in violation of the Children's Online Privacy Protection Act (COPPA). COPPA requires a website to obtain parental consent for collection of personal data from children under 13 years old.[16] The essence of personal data protection is accepted at least in principle across the world. For example, the EU General Data Protection Regulation (GDPR) provides specific protection for children's data, specifically providing clarity and information in simple language to aid in understanding the inherent risk associated with marketing ads, social media group luring and profiling by organizations.[17] In 2022, Google agreed to settle a class action lawsuit claiming that Google violated Illinois residents' privacy rights by not obtaining consent before using their biometrics information, a violation of the Illinois Biometrics Information Privacy Act (BIPA).[18]

In 2019, Google and its subsidiary YouTube paid a US$170 million civil penalty to the US Federal Trade Commission (FTC) and the US New York Attorney General to settle an allegation of illegally collecting and sharing personal information of children without their parent's consent in violation of COPPA.[19] Acting as a data recipient in that instance, Google ignored the children's privacy rights and discounted their concerns and risk realities because it had control of the information and understood the value and benefits of the children's biometric data to the development, relevance and profitability of its system.

Case 2—Facebook

Facebook may be the platform that collects the most information from its users based on its publicly available privacy policy information. It processes users' data across its data center globally, and it disburses and shares users' information with its trading partners worldwide. Facebook keeps information as long as it has a use for it. The enterprise's business model exploits the data value for profit, marketing and scholarly and applied research.[20]

Despite the wide-ranging collection of user data, Facebook points to a range of measures it takes to protect users' information. For example, the enterprise touts its use of encryption capabilities to maintain the integrity of data in motion. It also makes a point of not supporting government data collection backdoors, among other things.[21]

Data Exploitation

In July 2019, Facebook and the FTC reached a US$5 billion settlement of allegations that Facebook violated the FTC's 2012 Privacy Order. The allegation was that Facebook deceived its users about their capacity to control their data. Additional outcomes of the settlement were that Facebook would create multiple channels of compliance across its network and that it would ensure executives at Facebook were not only responsible and transparent, but also accountable for their privacy decisions.[22]

In 2011, Facebook and the FTC settled charges that it misused users' data. Facebook was barred from misrepresenting its privacy and security application, required to get affirmative consent from users, required to prevent access to user data 30 days after a user's account deletion, required to address privacy risk in the development and management of its new and existing products and services, and required to engage periodic independent audit evaluations.[23]

Case 3—Twitter

Twitter has described and categorized its data collection succinctly. As a result, its policy is simple and unambiguous. Twitter's data collection mechanism comprises the data users voluntarily provide to participate on the platform and the data collected from users, knowingly or unknowingly, through technology-assisted data collection methods[24] (that is, the information Twitter collects, primarily unbeknownst to users as they navigate or browse the site), and the cross-platform data collected by third parties.

In its safety and security section, Twitter, like other organizations, enumerates most of the uses for collected personal information, and most users agree to them—for example, the use of personal data for authentication and access.[25]

Data Exploitation

In May 2022, Twitter paid US$150 million to settle charges and was asked to cease profiting from data it deceptively collected from users. The settlement was paid because Twitter violated the 2011 FTC order. The enterprise deceptively obtained its 140 million users' information for target advertising instead of for increased security protection as it had promised. For example, users were asked to provide email addresses and phone numbers for two-factor authentication and to unlock their accounts due to suspicion of security breaches or malicious activities.[26]

In March 2011, the FTC finalized a settlement with Twitter for its role in deceiving users by failing to

The principles of the law of noncontradiction can be applied to understand why an entity would do everything to protect its own data while exploiting others' data.

safeguard their data. The problem was that Twitter failed to complete the information security and privacy confidentiality tasks, and it provided users with a false sense of security by offering private settings on its website, which did very little to safeguard users' data from hostile and malicious actors.[27]

Additional Examples

Under the GDPR, the European Union has issued more than 1,160 fines to organizations for privacy violations and noncompliance in fewer than five of its implementations—Amazon's receipt of a €746 million fine in 2021 being the highest.[28] Amazon's infringement in Europe relates to target advertising consent involving 10,000 people in 2018.[29] Yet, Amazon purports itself as a guardian of personal and enterprise data.[30]

Under Sections 18 and 34 of Australia's Consumer Law, Google and its affiliate, Google Australia Pty Limited, were fined AUD$60 million for misleading Android users. The users were not told that in addition to the location history setting, the web and app activity setting also enabled the collection of users' location data. [31]

Conclusion

The principles of the law of noncontradiction can be applied to understand why an entity would do everything to protect its own data while exploiting others' data. The fundamental principles of the union and intersection of sets scheme shows the complexity and dialectic struggle entities face in deciding when to protect or exploit data. Information privacy policies, regulations and enforcement mechanisms would better serve society if information privacy realities contradiction considerations were integral to policy formulation and legislative enactment from the onset and not tacked on as an afterthought.

The convergence of the unity of opposites, materialist dialectics and self-interest is the catalyst and driver of the information privacy realities contradiction theory. The unity of opposites exists naturally in human beings, individuals, organizations and nations; materialist dialectics identify the constant struggle of opposites; and self-interest determines which part of the opposite wins at a given time and under given circumstances. Therefore, the contradictory application of information privacy, compliance or violation is interest-based and universal.

Naturally, employees respond actively to what interests their managers. Thus, researchers and practitioners, including information privacy officers (e.g., chief information officers) and information privacy professional organizations, should develop and promote understanding of information privacy contradiction concepts and their implications in any information privacy discussions, education, training and awareness.

There is a need for further research into this phenomenon of information privacy contradiction because it is pertinent, omnipresent and universal.

Endnotes

1 US Department of Commerce, *Commerce Data Strategy: Fiscal Years 2021-2024*, USA, 2021, *https://www.commerce.gov/sites/default/files/2021-08/US-Dept-of-Commerce-Data-Strategy.pdf*

2 Kappel, K.; "Epistemological Dimensions of Informational Privacy," *Episteme*, vol. 10, iss. 2, 2013, *https://www.cambridge.org/core/journals/episteme/article/abs/epistemological-dimensions-of-informational-privacy/B71B5D6882E9325E1A7DB795AADB0607*

3 Horn, L.; "Contradiction," *The Stanford Encyclopedia of Philosophy (Winter 2018 Edition)*, 2018, *https://plato.stanford.edu/archives/win2018/entries/contradiction/*

4 Landauer J.; J. Rowlands; "Contradiction," Importance of Philosophy, 2001, *http://importanceofphilosophy.com/Metaphysics_Contradiction.html*

5 Venn J. I.; "On the Diagrammatic and Mechanical Representation of Propositions and Reasonings," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 10, iss: 59, 28 April 2009, *http://doi.org/10.1080/14786448008626877*

6 Ten.Info, "Top 11 Intelligence Agencies in the World 2022," 4 March 2022, *https://ten.info/top-intelligence-agencies/*

7 Tse-tung, M; *On Contradiction*, 1937, *https://www.marxists.org/reference/archive/mao/selected-works/volume-1/mswv1_17.htm*

8 *Ibid*.

9 *Ibid*.

10 Trotsky, L.; *In Defense of Marxism*, USA, 1942, *https://www.marxists.org/archive/trotsky/idom/dm/index.htm*

11 Coase, R.; "Adam Smith's View of Man," *The Journal of Law and Economics*, vol. 19, iss. 3, 1976, *https://www.journals.uchicago.edu/doi/abs/10.1086/466886*

12 Cropanzano, R.: B. Goldman; R. Folger; "Self-Interest: Defining and Understanding a Human Motive," *Journal of Organizational Behavior*, vol. 26, 15 November 2005, *https://onlinelibrary.wiley.com/doi/abs/10.1002/job.353*

13 Glasser, M.; *Choice Theory: A New Psychology of Personal Freedom*, HarperCollins, USA, 1998

14 Offor, P.; "Cybersecurity Intelligence: A Novel Information Security Threat Mitigation Approach," *Practice and Research*, November 2020, *http://repository.cityu.edu/handle/20.500.11803/1026*

15 Google, "Our Privacy and Security Principles," *https://safety.google/principles/*

16 Davis, W.; "Google Sued for Allegedly Collecting Students' Biometric Data," *Digital News Daily*, 3 April 2020, *https://www.mediapost.com/publications/article/349491/google-sued-for-allegedly-collecting-students-bio.html*

17 Intersoft Consulting, General Data Protection Regulation (GDPR), *https://gdpr-info.eu/*

18 Petkauskas, V.; "Google to Pay Residents $100 Million Over Privacy Violation," *Cybernews*, 6 June 2022, *https://cybernews.com/news/google-to-pay-residents-100-million-over-privacy-violation/*

19 Federal Trade Commission, "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," USA, 4 September 2019, *https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law*

20 Meta, "Privacy Policy," 26 July 2022, https://*www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0*

21 *Ibid*.

22 US Federal Trade Commission (FTC), "FTC Gives Final Approval to Modify FTC's 2012 Privacy Order With Facebook With Provisions From 2019 Settlement," 28 April 2020, *https://www.ftc.gov/news-events/news/press-releases/2020/04/ftc-gives-final-approval-modify-ftcs-2012-privacy-order-facebook-provisions-2019-settlement*

23 US Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers By Failing to Keep Privacy Promises," 2 9 November 2011, *https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises*

24 Offor, P.; "Why We Disclose Personal Information Despite Cybersecurity Risks and Vulnerabilities: Obligatory Passage Point Perspective," *International Journal of Smart Education and Urban Society*, vol. 9, iss. 4, 2018, *https://www.igi-global.com/article/why-we-disclose-personal-information-despite-cybersecurity-risks-and*-vulnerabilities/214053

25 Twitter, "Safety and Security, *https://help.twitter.com/en/safety-and-security*

26 US Federal Trade Commission, "FTC Charges Twitter With Deceptively Using Account Security Data to Sell Targeted Ads" 25 May 2022, *https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads*

27 US Federal Trade Commission, "FTC Accepts Final Settlement With Twitter for Failure to Safeguard Personal Information" 11 March 2011, *https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-accepts-final-settlement-twitter-failure-safeguard-personal-information*

28 Statista, "Largest Fines Issued for General Data Protection Regulation (GDPR) Violations as of July 2022," 2022, *https://www.statista.com/statistics/1133337/largest-fines-issued-gdpr/#statisticContainer*

29 Data Privacy Manager, "Luxembourg DPA Issues €746 Million GDPR Fine to Amazon," 30 July 2021, *https://dataprivacymanager.net/luxembourg-dpa-issues-e746-million-gdpr-fine-to-amazon/*

30 Amazon, "EU-US and Swiss-US Privacy Shield," *https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=202135380*

31 Australian Competition and Consumer Commission (ACCC), "Google LLC to Pay $60 million for Misleading Representations," 12 August 2022, *https://www.accc.gov.au/media-release/google-llc-to-pay-60-million-for-misleading-representations*