Open Access Library Journal
2025, Volume 12, e13554
ISSN Online: 2333-9721
ISSN Print: 2333-9705

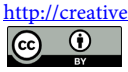
A Metric for Calculating the Extent of Non-Knowledge (Level) of Personal Privacy

Yair Oppenheim

School of Philosophy, Linguistics and Science Studies, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Tel Aviv-Yafo, Israel
Email: yairoppen@gmail.com

How to cite this paper: Oppenheim, Y. (2025) A Metric for Calculating the Extent of Non-Knowledge (Level) of Personal Privacy. *Open Access Library Journal*, **12**: e13554.
https://doi.org/10.4236/oalib.1113554

Received: May 2, 2025
Accepted: May 28, 2025
Published: May 31, 2025



Abstract

Personal privacy, in various aspects, has occupied humanity since the dawn of civilization, evolving and changing throughout human history. For the last two decades, the privacy issue has persistently remained the focus of public attention. Privacy, especially different aspects of personal privacy[1], continues to be at the center of public debate. This growing preoccupation with personal privacy stems from the great changes [1] that information and communication technologies (ICTs) have brought about in all walks of life during the last twenty years. The information revolution has made it possible to translate personal privacy into personal privacy information and, consequently, to discuss personal privacy in terms of personal privacy information. According to Shannon's information theory [2]. Information is measurable and quantifiable, so discussing personal privacy information allows us to replace a qualitative discussion of the definitions and essence of personal privacy with a quantitative discussion of the degree of one's privacy in each state of affairs. In this article, I will introduce a metric for quantifying and measuring personal privacy in each situation. This metric is based on the concept of "social distance" [3], which is equivalent to personal privacy. We will see how, with insights from information theory and the technological capabilities of ICTs, the abstract concept of social distance can be quantified and measured.

Subject Areas

Complex Network Models

Keywords

Personal Privacy, Personal Privacy Basic Components, Deep and General

[1]Personal privacy is the type of privacy that applies to individual humans, in contrast to general privacy, which also applies to organizations, corporations and agencies.

Personal Privacy, Social Distance, Metric for Calculating the Extent of Non-Knowledge of Personal Privacy Information

1. Introduction

Many attempts have been made to redefine personal privacy. However, as Daniel Solove shows [4] [5], none of these definitions are complete and exhaustive in describing the phenomenon of personal privacy [6]-[9]. Several questions remain unclear: What is privacy as a concept? Where and to what does it apply? Where does the private sphere end and the public sphere begin? Where does privacy stand in terms of other concepts, such as freedom, autonomy, and liberty? How to balance individual human rights against the public's right to know? Must a state reveal potential threats to its security? And how should it all be regulated in this age of information and communication technologies, which follow us wherever we go and whatever we do? The failure to define personal privacy makes it very difficult to formulate social norms or legal regulations that would protect it from being violated by individuals, corporations, social organizations, and governments in this era of the information revolution.

In this article, I propose a way to overcome the inability to define privacy by changing the approach and handling the issue of personal privacy using quantitative tools. These tools may be able to provide a solution where qualitative and legal tools fail.

I will begin by breaking personal privacy down to its basic components: body, mind, private space, actions, property, external entities, relationships with external entities, autonomy, identity, and anonymity. These basic components are related to each other, and their combination defines personal privacy as a whole. Each of the basic components of privacy carries elements of information. Together, the elements of information carried by all the basic components of privacy make up all the personal information about us. Based on this, we can **replace the discussion of personal privacy with a discussion of personal privacy information**—a concept that is measurable and quantifiable, according to Claude Shannon's information theory [2]. The digitization of personal information is what allows ICTs to store, process, analyze, and disseminate personal privacy information.

My metric for calculating the extent of non-knowledge of personal privacy information is based on the concept of social distance, described by Georg Simmel as the effect of the information and knowledge people have about each other [3].

2. The Six Conceptions of Personal Privacy

According to Solove [10], six major conceptions capture the main ideas in the discourse about privacy. These conceptions are closely related and sometimes overlap, and together, they cover the notion of privacy in its modern Western liberal interpretation. The six conceptions are as follows: 1) the right to be let alone

[11] —Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; 2) limited access to the self [12] —the ability to shield oneself from unwanted access by others; 3) secrecy [13] —the concealment of certain matters from others; 4) control over personal information [14] —the ability to exercise control over information about oneself; 5) personhood [13] —the protection of one's personality, individuality, and dignity; and 6) intimacy [15] —control over, or limited access to, one's intimate relationships or aspects of life [15].

3. The Basic Components of Personal Privacy

Out of the six conceptions of privacy discussed by Solove, I was able to extract the following **basic components of privacy [16]**:

Private space: The physical and virtual areas where one has privacy. Private space has a static physical aspect, which is one's physical place of residence, and a dynamic physical aspect, which can be envisioned as an envelope or bubble that surrounds and follows one wherever one goes.

Body: One's body, which includes physical characteristics such as appearance, height, weight, strength, health, senses, and medical conditions, as well as the brain and nervous system, which are often perceived as carriers of mental properties.

Mind: The abstract part of one's person, which includes one's thoughts, feelings, desires, fears, self-perception, memories, and other mental and psychological elements. Only in the modern era was the concept of personal privacy extended to include the mental and psychological realm.

Actions: The things one does and the way one behaves in the world, including things one says or writes, one's physical movements, and one's social and intimate relationships (who one has social or intimate relations with, the nature, frequency and intensity of the relationships, whether they include expression of feelings and/or exchange of information, etc.). In other words, all of one's lifelong behaviors and acts, including those related to other people. One's actions and behaviors are also a manifestation and realization of personal decisions, and, as such, are an expression of individual autonomy, or lack thereof, if one is not acting of one's own free will.

Property: One is the sole owner of one's body; one's mind, one's personal physical space in which one can do whatever one likes, and the abstract products of one's mind, such as thoughts and memories.

External entities: Other players in the system of balances between the protection and violation of one's privacy. Such entities can be human—other individuals or political, social or commercial organizations (e.g., commercial companies or governments) —or they can be social networks, like Facebook or Google. Some of them are one's confidants who possess confidential private information about one, for example, healthcare providers who possess information about one's physical and mental health, lawyers who possess confidential legal information, banks who possess confidential financial information, and intimate partners who possess intimate information about one.

Relationships with external entities: The nature of one's relationships with other entities (whether the relationship is intimate, familial, economic, legal, work-related, subordinate, professional or social), including the power relations between the parties and the intensity of the relationships (the importance attributed to the relationship by each of the parties, the emotional strength of the relationship, the extent of mutuality, the amount of time invested in it, etc.).

Autonomy: An individual's capacity for self-determination or self-governance, the ability to decide for oneself, without any external interference, regarding one's own body and mind [16]. Philosophers make a distinction between personal autonomy, moral autonomy, and political autonomy. Moral autonomy, usually traced back to Kant, is the capacity to deliberate and to give oneself the moral law, rather than merely heeding the injunctions of others; personal autonomy is the capacity to decide for oneself and pursue a course of action in one's life, often regardless of any particular moral content; and political autonomy is the property of having one's decisions respected, honored, and heeded within a political context. According to the liberal democratic approach, all three are part of an individual's privacy. The individual makes moral decisions for themself and is responsible for their consequences—good or bad; that includes faith and religious practices, which in modern society are considered people's private business. The individual interacts with and affects reality as an independent and autonomous agent, and representative democracy is based on this autonomy of individuals to be political agents who elect their representatives in a process of free and secret elections to ensure the autonomy and authenticity of their choices.

Identity: The philosophical question of human identity has concerned humanity since the days of Plato [17]. It has been phrased in many ways, [18] such as "Who am I?" or the Socratic "know thyself", or Paul Gauguin's "Where do we come from? What are we? Where are we going?".

Identity is a vague and complex concept. In this article, I make a distinction between "selfhood" and "identity", which I define as the outer representation of one's inner self. According to the liberalist approach, selfhood is a product of one's unique individuality [19], for even though every individual is made up of the same universal building blocks [20] such as common human physiology, genetics[2] and cognitive abilities, the combination of those, together with every person's unique history, is what creates each individual's unique selfhood. Therefore, a person's identity is also unique, as it represents that person's unique selfhood. This does not mean that identity is static and unchanging; it is only that it can always be associated with one unique individual. An individual can have multiple identities, each of which either represents a different part (or parts) of the same "core self", or an altogether different self or selves. The different identities are time- and context-dependent, and not necessarily distinct from each other. Some of them may coexist simultaneously, while others replace previous identities.

[2]Like the way every human's DNA is made up of the same four basic units, but each person's complete genome is unique.

The new category of identities that was born in the age of ICTs can be collectively called "online identities". Those are identities one creates or assumes in the virtual world. Every person who is connected to the Internet has at least two identities at the same time: their offline identity and their online identity [17]. Online identities can be divided into two sub-categories: identities one creates for oneself on social media and in various Internet applications, and user identities (profiles) created by large Internet companies to use as business aid. Online identities created by Internet companies do match the choices, experiences, and actions of specific real-life individuals, and change as the Internet company collects more and more information about the individual in question. Many times, e.g., on Tinder, Amazon, Facebook, and other similar applications, they are added to the online identity the individual themself knowingly created.

Even though an individual can have more than one online identity at the same time, and that these may be very different from one another, they can still be associated with and traced back to one physical person with a continuous memory and experience [21]. In the age of ICTs, this is done employing constant monitoring of people through IoT technologies. Neither of those systems alone is adequate for making the associations required to trace all the different identities back to a specific person, but using several systems to cross-reference data can reveal the one individual behind the multiple online identities.

Anonymity: As Michael Birnhack has noted, anonymity is a concept that can be hard to define. The literal meaning of the word "anonymous" is "nameless", and it usually means doing something without identifying oneself [22]. Helen Nissenbaum describes anonymity as the inability to get to (or at) a person, *i.e.* to associate elements of information or actions manifested in the physical world with a specific individual [23].

In the age of ICTs, the claim for anonymity has been extended to:

- Sending electronic messages (e.g., emails) without the sender's (and sometimes also the addressee's) name being revealed.
- Participating in virtual interactions (chat rooms, online gaming, online dating services, e-commerce) without your real name being known to other participants.
- Purchasing goods and services online using virtual currency (e.g., bitcoin) and without giving out your name.
- An ability to visit any website without having to divulge your identity.

In general, ICTs are making anonymity almost impossible [24]. The information collected about us by every ICT we use is being aggregated in interconnected databases and analyzed using advanced technology. This is an actual violation of personal privacy: biometric data pools add up physical and mental properties and characteristics, enabling the association of various online profiles with specific people. Combined use of technological means of surveillance and monitoring eventually renders multiplicity of identity practices useless.

Table 1 illustrates the relationship between the six conceptions described by Solove and the categories of information carried by the basic components of personal privacy.

Table 1. The relationship between the six conceptions described by Solove and the categories of information.

		Solove's conceptions of privacy							
		The right to be let alone	Limited access to the self	Secrecy	Control over personal information	Personhood	Intimacy	Information obtained directly or indirectly	Information category No.
Information categories carried by the basic components of privacy	Private space information	V	V				V	Directly	1
	Body-related information	V	V			V	V	Both	2
	Mind-related information	V	V			V	V	Indirectly	[3]
	Information about actions	V	V	V	V		V	Both	4
	Property information	V			V	V		Directly	5
	Information about external entities	V	V	V	V		V	Both	6
	Information about relationships with external entities	V	V	V	V	V	V	Both	7
	Information about the values that guide decisions and actions (autonomy information)		V	V	V	V	V	Indirectly	8
	Anonymity information	V	V	V	V	V		Both	9
	Identity-related information			V	V	V		Both	10

4. Numeric Calculation of the Extent of Non-Knowledge of Personal Privacy

According to Georg Simmel, social distance is the effect of the information and knowledge people have about each other [25]. This is the formal definition of the private sphere in terms of information and knowledge, which Alan Westin also calls "social distance". For this metric, I will replace the term "social distance" with "extent of non-knowledge of personal information" to allow me to measure the level of personal privacy in a given situation.

The metric is based on the basic categories of personal privacy information. (See Table 2)

Table 2. Information category vs Information elements.

Information category	Information elements	Information index
Private space information	Information related to our private space as defined by the social norms and regulations.	1
Body-related information	Body appearance, physical characteristics, physical location, "passport identity" information.	2
Mind-related information	Character traits, mental properties, preferences (including gender/sexual preferences).	3
Information about actions	Information about our habits, deeds, behavior and routine.	4
Property information	Information about our physical and/or intellectual property.	5
Information about external entities	Information about other entities that are nodes in our network and have information about us.	6
Information about relationships with external entities	Information about our relationships with other entities: the existence of a relationship, the nature and intensity of the relationship.	7
Autonomy information	Information about what can diminish our autonomy, *i.e.*, our ability to be the exclusive decision makers regarding our own thoughts, feelings, actions, desires and relationships with others (including relationships with government and corporate entities).	8
Anonymity information	Any piece or pieces of information that can – alone or when combined – breach our anonymity, i.e., our ability to remain unidentified in the public sphere.	9
Identity-related information	Information about our various identities.	10

4.1. Metric Definitions

PI (Personal Information) —All the information you know about yourself.

SI (Social Information) —All the information about you that is known to the public.

Based on these, the extent of non-knowledge of personal information (all the information about you that is unknown to the public) is $EP = PI - SI$.

This is the mathematical formulation of social distance.

The social distance of any given individual i consists of the following parameters:

PI_i^j is the knowledge individual i has about themself regarding information category j (e.g., i's knowledge about i's own body). Let its range be $0 \leq PI_i^j \leq 1$.

The two extreme cases are $\boldsymbol{PI}_i^j = 1$, *i.e.*, individual i knows everything about their body (including physical flaws, complete health state, and latent genetic features), and $PI_i^j = 0$, *i.e.*, individual i knows nothing about their body. Both are very unlikely, though theoretically possible.

WP_i^j is the significance (weight) category j has for individual i. It is, of course, subjective, varies from one individual to another, and depends on context and

social norms; still, it can be assigned an exact value under given circumstances. Its range is $0 \le WP_i^j \le 1$.

$SI(l)_i^j$ is the knowledge another individual *l* or entity *l* has about individual *i* regarding information category *j* (e.g., somebody else's knowledge about individual *i*'s body, including physical flaws, complete health state, and latent genetic features). There can be two kinds of "others": a confidant or a public organization/Internet company. The range of this parameter is also $0 \le SI(l)_i^j \le 1$, the extreme cases being $SI(l)_i^j = 1$ (the other *l* has all the information about category *j* of individual *i*) and $SI(l)_i^j = 0$ (the other *l* has no information at all about category *j* of individual *i*). Both are very unlikely, though theoretically possible. For simplicity's sake, the metric ignores the distinction between the two different kinds of "others".

4.2. The Metric

Based on the above definitions, we can calculate, for example, the extent of the non-knowledge of Facebook (*l* – other) about individual *i*, using the following formula:

$$EP(i,l) = \sum_{j=1}^{10} \left(WP_i^j \left(PI_i^j - SI(l)_i^j \right) \right)$$

Although the metric is well-defined, it may be difficult to use in practice. This difficulty can be overcome by using an *N*-size representative sample of "others," which would include confidants, Internet companies, etc. *N* can be relatively small, as long as it provides an accurate representation of the public and takes into consideration the extent of knowledge held by dominant social entities, such as government organizations and giant corporations like Google, Facebook, and Amazon, which make use of people's private information.

The *M* sample size should be big enough to be a representative sample of individuals with the given characteristics. It can be compiled from multiple suitable big data pools. The sampled group's average extent of non-knowledge should be calculated as follows:

$$DI = \frac{1}{M} \left(\sum_i \sum_l EP_i \right) \text{ with } i = \{1,2,\cdots,M\}, \quad l = \{1,2,\cdots,N\}$$

This will provide a numeric value that can serve as a metric for measuring information privacy level. The metric can be used by regulatory organs and legal institutions to measure the extent to which Facebook, for example, meets the GDPR requirements.

4.3. A Numerical Example

Let us assume, for simplicity's sake, that every $WP_i^j = 1$ for every individual *i* and for every category *j* of personal privacy. *SI*(*l*) represents the knowledge the Internet (e.g., social media, web applications, cloud databases) has about average individual *i*.

The calculation is built from the bottom up: I divided each category of personal privacy information into several subcategories and asked (prompted) ChatGPT and Gemini to rank each on a scale of 0 - 1. Then, I made an average of the scores obtained from the two sources. The intermediate calculations can be found in the Excel file [26]. The ChatGPT prompts are described in the Appendix [27]. Without loss of generality, I assume the results are true for average individuals i in the US and the European Union.

The final results are presented in the two summary tables below [28]: one for the US and one for the EU. The scores represent the extent of knowledge or non-knowledge of personal privacy information. (See **Table 3** and **Table 4**)

Table 3. The US summary table.

j index	Information category	PI - Personal information	$SI(I)$ - Social information	EP_i^j
1	Private space information	0.48	0.65	−0.18
2	Body-related information	0.58	0.48	0.10
3	Mind-related information	0.77	0.69	0.08
4	Information about actions	0.62	0.84	−0.22
5	Property information	0.69	0.78	−0.09
6	Information about relationships with external entities	0.65	0.82	−0.17
7	Information about external entities	0.63	0.82	−0.19
8	Autonomy information	0.49	0.34	0.15
9	Anonymity information	0.51	0.66	−0.15
10	Identity-related information	0.505	0.655	−0.15
	Average	0.54	0.61	−0.07

Table 4. The EU summary table.

j index	Information category	PI - Personal information	$SI(I)$ - Social information	EP_i^j
1	Private space information	0.58	0.43	0.15

Continued

2	Body-related information	0.44	0.37	0.07
3	Mind-related information	0.75	0.58	0.17
4	Information about actions	0.72	0.70	0.02
5	Property information	0.76	0.74	0.02
6	Information about relationships with external entities	0.73	0.75	−0.02
7	Information about external entities	0.70	0.79	−0.09
8	Autonomy information	0.69	0.59	0.10
9	Anonymity information	0.46	0.61	−0.15
10	Identity-related information	0.65	0.63	0.02
	Average	0.65	0.62	0.03

From this AI-assisted ranking of the average degree of privacy in the US and the EU, the following conclusions can be drawn:

- The average personal privacy in Europe is 3%, while in the US, the average personal privacy is −7%. That is, in the US, personal privacy is negative, which means that the Internet (e.g., social media, web applications, and cloud databases) has more information about the average individual than the individual has about themself. In contrast, in the EU, the average personal privacy is positive, which means that the average individual knows more about themself than the web knows about them. These differences are due to the differences in privacy protection regulations between the US and the EU. In the EU, these regulations are stronger than in the US. Moreover, the EU government is more inclined to enforce the regulations by finding Internet companies and restricting governments' ability to collect information about their citizens.
- In the categories **Information about relationships with external entities**, **Information about external entities**, and **Anonymity information**, both in the US and in the EU, personal privacy is negative, which means that the Internet has more information about the individuals themselves. It should be noted that these are categories that contain, one way or another, information about the individual's relationship with others (other individuals or public and government organizations). It is therefore natural that the privacy of information from these categories is almost impossible to maintain in the age of ICTs.

- In the categories **Private space information**, **information about actions**, **Property information**, and **Identity information**, the personal privacy of the average American individual is negative, which indicates the weakness of the regulations whose role is to maintain legal privacy in the US, and/or the failure of the legal system to implement those regulations.
- Although the overall level of personal privacy is very low both in the US and in the EU, the category of **Autonomy** receives a positive score in both (15% and 10% respectively), and is rated slightly higher than most of the other categories. This is a positive sign of the resilience of democracies, because it indicates the degree of ineffectiveness of fake news that are being spread all over the Internet and social media and shows us that the average individual in the US and the EU manages to maintain their autonomy.

In general, in-depth surveys in focus groups are needed to confirm or refute these findings. However, the workable and reliable measurement tool that has been presented here makes it possible to measure in practice, in each state of affairs, the general level of personal privacy or a specific component(s) of privacy. This tool can also be useful for periodic assessment of trends (improvement or deterioration) in the state of personal privacy in general or in a specific component(s) of privacy.

5. Conclusions

In the ICT age, for the first time in history, personal privacy can be translated into information. Information, by nature, is measurable and quantifiable [2]. These characteristics of information make it possible to construct quantitative indicators for a given state of affairs and thus transform the debate around personal privacy from a qualitative discussion focused on the definitions of personal privacy to the measurement of the level of personal privacy of an individual or a company.

In this article, I have introduced a metric that can help quantify and measure the degree (level) of personal privacy. This metric is based on the concept of "social distance" and the idea that personal privacy can be broken down to its basic components. The metric can be used by regulatory agencies to measure **violation of personal privacy by entities such as Internet companies or governments.**

The example presented in this article numerically supports the common intuition that in the age of ICTs, personal privacy as it is defined in the liberal Western society is almost completely wiped out.

The metric presented here can help assess the degree of violation of a single person's privacy, a group of people, or an entire society, in general or about one or more basic components of privacy.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Toffler, A. (1980) The Third Wave. Morrow, 17.

[2] Shannon, C.E. (1948) A Mathematical Theory of Communication. *Bell System Technical Journal*, **27**, 623-656. https://doi.org/10.1002/j.1538-7305.1948.tb00917.x

[3] Simmel, G. (1910) How Is Society Possible? *American Journal of Sociology*, **16**, 372-391. https://doi.org/10.1086/211904

[4] Solove, D.J. (2009) Understanding Privacy. Harvard University Press, 1-2.

[5] Nissenbaum, H. (2009) Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, 16. https://doi.org/10.1515/9780804772891

[6] Schoeman, F.D. (1984) Privacy: Philosophical Dimensions. In: Schoeman, F.D., Ed., *Philosophical Dimensions of Privacy*: *An Anthology*, Cambridge University Press, 3.

[7] Laurie, G. (2002) Genetic Privacy: A Challenge to Medico-Legal Norm. Cambridge University Press, 6. https://doi.org/10.1017/cbo9780511495342

[8] Hongladarom, S. (2016) A Buddhist Theory of Privacy. Springer, 16.

[9] Gavison, R. (1980) Privacy and the Limits of Law. *The Yale Law Journal*, **89**, 421. https://doi.org/10.2307/795891

[10] Solove, D.J. (2002) Conceptualizing Privacy. *California Law Review*, **90**, 1088-1154. https://doi.org/10.2307/3481326

[11] https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[12] Gavison, R. (1980) Privacy and the Limits of Law. *The Yale Law Journal*, **89**, 433.

[13] Solove, D.J. (2002) Conceptualizing Privacy. *California Law Review*, **90**, 1107.

[14] Fried, C. (1968) Privacy. *The Yale Law Journal*, **77**, 475-493. https://doi.org/10.2307/794941

[15] Gerstein, R.S. (1978) Intimacy and Privacy. *Ethics*, **89**, 76-81. https://doi.org/10.1086/292105

[16] Yair, O. (2024) Personal Privacy in the Age of the Internet.

[17] "Autonomy", Internet Encyclopedia of Philosophy. https://iep.utm.edu/autonomy/

[18] Floridi, L. (2011) The Informational Nature of Personal Identity. *Minds and Machines*, **21**, 549-566. https://doi.org/10.1007/s11023-011-9259-6

[19] Levin, I. (2016) Cyber-Physical Systems as a Cultural Phenomenon. *International Journal of Design Sciences and Technology*, **22**, 67-80.

[20] Rabi, L. (2009) The Burden of Individuality: The Origins of the Modern Ideal of Individuality. Pardes, 255. (In Hebrew)

[21] Garcia, J.J.E. (1988) Individuality: An Essay on the Foundation of Metaphysics. State University of New York Press, 234.

[22] Schechtman, M. (2007) Stories, Lives, and Basic Survival: A Refinement and Defense of the Narrative View. In: Hutto, D., Ed., *Narrative and Understanding Persons*, Cambridge University Press, 155-178. https://doi.org/10.1017/cbo9780511627903.009

[23] Birnhack, M.D. (2010) Private Space: The Right to Privacy, Law and Technology. Bar-Ilan University, 269. (In Hebrew)

[24] Nissenbaum, H. (1999) The Meaning of Anonymity in an Information Age. *The Information Society*, **15**, 141-144. https://doi.org/10.1080/019722499128592

[25] Schneier, B. (2016) Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton and Company, 4-42.

[26] Simmel, G. and Wolff, K.H. (1950) The Sociology of Georg Simmel. Free Press, 312.

[27] For the Full Excel File.
https://onedrive.live.com/edit?id=CAC67BD0F9AD4A17!s19064f3a06d64bffaea3c3187d97c39f&resid=CAC67BD0F9AD4A17!s19064f3a06d64bffaea3c3187d97c39f&cid=cac67bd0f9ad4a17&ithint=file%2Cxlsx&redeem=aHR0cHM6Ly8xZHJ2Lm1zL3gvYy9jYWM2N2JkMGY5YWQ0YTE3L0VUcFBCaG5XQnY5THJxUERHSDJYdzU4Qk1iR-zRBLXZlM1JsX0FfanRYSkdiYlE_ZT12VFc5TWk&migratedtospo=true&wdo=2

[28] ChatGPT Prompts Appendix.
https://1drv.ms/w/c/cac67bd0f9ad4a17/ER-rHn7bWXp9KnjY9PCXyBhQBILgm0FKA6fJwV1BROWEueg?e=ak970B