International Journal of Science Academic Research
Vol. 06, Issue 06, pp.10231-10237, June, 2025
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

PERSONAL PRIVACY AS GAME THEORY MODELS

***Dr. Yair Oppenheim**

Linguistics and Science Studies, School of Philosophy, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University,Israel

Received 12th April 2025; **Accepted** 16th May 2025; **Published online** 30th June 2025

Abstract

The balance between individuals' interest in protecting their private information and the interests of other entities (other individuals, confidants, Internet companies, corporations, and government agencies) has been disrupted in the age of ICTs [1].I suggest using game theory models to find new points of balance, which I will now describe in the following models.

Keywords: Personal Privacy, Game Theory, Nash equilibrium, Players, Deep personal privacy, General personal privacy information, GDPR.

INTRODUCTION

Why use game theory models

In the age of ICTs, our personal information has become a commodity in the hands of players in the commodity market [2]. Those players use individuals' personal information to maximize their profits. The said individuals, being nodes in the network, seemingly give out their private personal information for free; they provide it every time they make an online purchase, receive medical treatment, pay their taxes, search for information on Google, or just browse the web for fun. This state of events justifies using game theory models (exemplars) to understand the rationale behind network players' decisions to violate personal privacy. That understanding will allow us to come up with alternatives that may affect the players' considerations and lead to reduced violation of personal privacy. For each model I present here, I will describe possible alternatives that may be able to prevent or reduce personal privacy violations.

Terms and Theorems

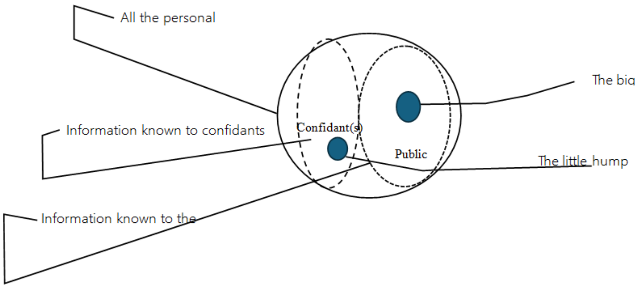
- The players are selfish and rational: They act out of rational considerations of gain and loss and solely to maximize their payoff.
- Perfect information game: At every stage of the game, every player has full knowledge of all the stages of the game, of all the players' previous moves, and of the strategies each player may use during the game.
- Non-cooperative game: A game in which players cannot form alliances or agree on solutions (equilibria). Each player is acting selfishly and rationally to maximize its payoff.
- Strategy: A player's strategy is what guides its actions and choices throughout the game, telling it what to do for every possible situation [3].
- Nash equilibrium: A situation where no player can gain by changing its strategy (the strategy vector $S^* = (s_1^* \dots s_i^* \dots s_n^*)$ is a Nash equilibrium if sticking with s_i^* is the best option for player *i* [4].
- Dominant strategy: A player's strategy that is equal or superior to every other strategy available to that player [5].
- Pure and mixed strategies: A pure strategy is any strategy S_i used by player *i.* A mixed strategy is the assignment of a probability between *0* and *1* to each of the pure strategies available to player *i* – let us call them *j*, *m*, and *n* – so that $p_j + p_m + p_n = 1$ [6].

Setting and Moves

The move options – to share or to withhold personal information – are based on the possession of the said personal information by each of the players. The information possession options are:

- Information possessed solely by the individual (deep personal privacy);
- Information possessed by the individual and shared by them with a confidant (general personal privacy);
- Information possessed by others who are not confident (personal information that is known publicly);
- Information possessed solely by the confidant, and not by anyone else (the little hump);
- Information possessed by the public, but not by the individual in question (the big hump).

This can be graphically represented as follows:



The outermost oval represents all the personal information about an individual, the dashed oval represents the personal information known to confidants, and the dotted oval represents the personal information that is known to the general public.

Corresponding Author:** ***Dr. Yair Oppenheim
Linguistics and Science Studies, School of Philosophy, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Israel.

Deep personal privacy information (all the information known only to the person in question) is all the area outside the dashed and dotted ovals.

General personal privacy information is the entire area of the outermost oval minus the area of the dotted oval.

Exposure of personal privacy information creates the "humps" – information about the individual possessed by confidants and/or the general public, but not by the individual themself. On the graph, the humps are represented by the two smaller ovals inside the dotted and dashed ovals.

The general model game description

Basic conditions

a. The game has three players:

- An individual (Player I), who possesses their deep privacy information.
- A confidant (Player II), who possesses Player I's general privacy information and "little hump" information.
- Internet companies (Player III), which possess Player I's information that is publicly known as well as "big hump" information.

b. The set prices are as follows:

- The free market price of a unit of information is $*x*;
- The fine for violating Player I's privacy is $*y*.[1]

c. The game may have one or more rounds. Each round is independent of the previous ones, and therefore, in each round, a player may only choose one of the options available to them.

d. For the sake of convenience, let the aforementioned information possession options be numbered as follows:

- Information possessed solely by the individual – 1
- Information possessed by the individual and shared by them with a confidant – 2
- Information possessed by others who are not confidants – 5
- Information possessed solely by the confidant – 3
- Information possessed by the public, but not by the individual in question – 4

This matrix reflects the actual current state of events concerning online privacy, and means the following:

e. The individual (Player I) gives up their privacy for free – unless we consider the services they get from their confidants, and especially from Internet companies (in the form of "free" apps), to be consideration.

f. The confident (Player II) may gain from using Player I's privacy information, but may be fined for selling elements of Player I's private information, which would be a violation of its ethical and legal obligations to protect the confidentiality of Player I's personal information.

g. Player III (Internet companies) may freely trade in individuals' private information. This assumption is in line with the analysis of surveillance capitalism presented in Chapter 9.

h. One way to balance out the interests of the different players in this game would be to fine Internet companies for privacy violations, as stipulated in the GDPR.

i. All the values in the payoff matrices discussed in this appendix are probable examples given based on subjective assessment. To learn the actual value of personal information for the different players included in this matrix, future researchers may survey players from the different categories to obtain their assessment of the payoffs in the models provided here. My underlying assumption, without loss of generality, was that all the basic components of privacy have the same value for Player I, and the same (though different from Player I's) value for Player II.

Based on this general payoff matrix, we can define three equilibrium games:

1. Individual vs confidant
2. Individual vs Internet company
3. Confidant vs Internet company

Game Model 1: Individual vs Confidant

The personal information protection game scenario between an individual and their confidant is as follows:

The individual and the confidant both possess the individual's private personal information. The individual shares this information with the confidant to enjoy its services (e.g., medical care, legal counselling, financial counselling, or customized recommendations for products).

e. The basic payoff matrix of the game:[1]

		Player I			Player II			Player III		
Information source	Information destination	Value of privacy loss	Gain for privacy loss	Total	Fine for source node privacy loss	Gain for source node privacy loss	Total	Value of source privacy loss	Gain for source privacy loss	Total
1	2	$-I_{12}\cdot x$	0	$-I_{12}\cdot x$	$-I_{12}\cdot y$	$I_{12}\cdot x$	$I_{12}\cdot x - I_{12}\cdot y$			
1	5	$-I_{15}\cdot x$	0	$-I_{15}\cdot x$					$I_{15}\cdot x$	$I_{15}\cdot x$
2	5				$-I_{15}\cdot y$	$I_{15}\cdot x$	$I_{25}\cdot x – I_{25}\cdot y$		$I_{15}\cdot x$	$I_{15}\cdot x$
3	1	$I_{31}\cdot x$	0	$I_{31}\cdot x$		$I_{31}\cdot x$	$I_{31}\cdot x$			
3	4				$- I_{34}\cdot y$	$I_{34}\cdot x$	$I_{34}\cdot x - I_{34}\cdot y$		$I_{34}\cdot x$	$I_{34}\cdot x$
4	1	$I_{34}\cdot x$	0	$I_{34}\cdot x$					$I_{34}\cdot x$	$I_{34}\cdot x$

[1] In this game, only Player I's privacy can be violated.

The confidant commits to protect the information and not to share it with any third parties – a commitment that is often enforced by law (as in the case of doctor-patient confidentiality or attorney-client privilege) or at least required by social norms (e.g., sharing of intimate information between sexual partners). Nevertheless, the confidant is tempted to trade the individual's personal information with third parties, because, as I have shown, personal information is a valuable resource that may bring the confidant considerable profit. In view of this relationship, let us analyze the "game" between the two, where each party chooses the strategy that best serves its interests, and look for equilibria.

The Game Setting

For the basic conditions of the game, see section "Basic Conditions".

Players: Player I is an individual who possesses private personal information;[2] Player II is a confidant in whom Player I sees a candidate for sharing their private personal information with.[3]Available **strategies:** Player I (the individual) has two possible strategies: to share their information in full, or to share it in part.[4] Player II (the confidant) also has two possible strategies: to maintain the confidentiality of Player I's information or to trade it.[5]

The Game's Payoff Matrix

Let the general payoff matrix be:

	Information value for Player I		Information value for Player II	
	Player I shares full information	Player I shares partial information	Player I shares full information	Player I shares partial information
Player II maintains information confidentiality	(a)	(b)	(c)	(d)
	1	0.5	1	0.5
Player II sells the information	(e)	(f)	(g)	(h)
	-1	-0.1	0.9	0.2

Payoff matrix justification:

For Player I:

If Player II maintains the confidentiality of Player I's information, Player I will benefit the most from sharing full information with Player II: in our example, it will allow the doctor Player II to provide optimal medical care to the patient Player I. Therefore, the information value is *1*. If Player I shares only part of their information, they will receive care that is less than optimal, and therefore, the information value is only *0.5*.

If Player II violates their confidentiality commitment, Player I will suffer harm (e.g., their insurance company will raise their life insurance premium as a result) at a value of *-1* if they shared their full information, or *-0.1* if they only shared part of their information.

For Player II:

If Player II received full information from Player I, maintaining confidentiality allows them to fully realize their abilities (in our example, provide the best medical care, which would earn them a good reputation); therefore, the information value is *1* for them as well. If they received partial information, the value of that information is only *0.5*.

Violating Player I's confidentiality in case of possessing full information gives Player II a value of *0.9* (the value of selling the information). In case of partial information, the value of sales is only *0.2*.

Importantly, when Player II is choosing a strategy, they cannot know whether Player I has given them full or partial information. Only Player I can know that.

Based on this, we can calculate a more specific payoff matrix for each of the players. Let us mark Player I's payoffs as X_{ij}, with $i = 1$ meaning provision of full information by Player I, $i = 2$ meaning provision of partial information, $j = 1$ meaning maintaining of confidentiality by Player II, and $j = 2$ meaning breach of confidentiality. Similarly, let us mark Player II's payoffs as Y_{ij}. I am assuming a confident will always sell the information it has received to maximize its profit [7].

The game payoffs will be as follows:

$$X_{11} = (a) = 1$$
$$X_{12} = (a) + (e) = 1 + (-1) = 0$$
$$X_{21} = (b) = 0.5$$
$$X_{22} = (b) + (f) = 0.5 + (-0.1) = 0.4$$

$$Y_{11} = (c) = 1$$
$$Y_{12} = (c) + (g) = 1 + 0.9 = 1.9$$
$$Y_{21} = (d) = 0.5$$
$$Y_{22} = (d) + (h) = 0.5 + 0.2 = 0.7$$

For convenience, let us display this payoff matrix in tabular form:

Player I's payoff matrix:

	Player I shares full information	Player I shares partial information
Player II maintains confidentiality	1	0.5
Player II breaches confidentiality	0	0.4

Player II's payoff matrix:

	Player I shares full information	Player I shares partial information
Player II maintains confidentiality	1	0.5
Player II breaches confidentiality	1.9	0.7

The game has a pure strategy Nash equilibrium. Player II has the dominant strategy: whatever the case, breaching Player I's confidentiality pays off. If Player I chooses the strategy of sharing full information, and Player II maintains its confidentiality, both will have a payoff of *1*. However, breaching confidentiality will increase Player II's payoff to

[2] For the sake of this example, let Player I be a patient.

[3] Let Player II be a doctor.

[4] The motive for sharing full information is clear – the desire to receive better service and help from the confidant (e.g., medical care). Choosing to share only part of the information may be based on a belief that it will better serve your interests: e.g., if you do not disclose all your financial information, you may be able to get better loan terms.

[5] Choosing to maintain confidentiality usually stems from legal or normative obligation, while choosing to sell the information is usually motivated by the desire to make a profit of it.

1.9. Therefore, the best strategy for Player I will be to initially share only partial information, to secure a payoff of at least *0.4*. But even then, it still pays off for Player II to breach confidentiality, as their payoff will be *0.7* instead of *0.5*. Since neither player can do better than that, this is the Nash equilibrium of this game.This is an example of a one-time game in which distrust between an individual and their confidant leads to both of them not getting the optimal outcome they might have had if they had maintained general privacy. The cost of privacy violation is $1 - 0.4 = 0.6$ for Player I, and $1 - 0.7 = 0.3$ for Player II.We can assume there will also be a social cost for violating privacy in this game: $0.6 + 0.3 = 0.9$. This supports the argument that maintaining personal privacy serves society even more than it serves the individual.

Game Model 2: Individual vs Internet Company

In this game scenario, the individual and the Internet company both possess the individual's private personal information. The individual shares this information with the Internet company (a navigation app like Waze, a social network like Twitter, or a search engine like Google) to enjoy the services it provides. The Internet company commits to protecting its users' information privacy and usually asks its users to affirm they have read and agree to the company's privacy policy.

The Internet company must comply with its declared information security policy; however, it is sorely tempted to trade the individual's personal information with third parties using loopholes in the said policy, because, as explained earlier, personal information is a valuable resource that can bring it considerable profit. Because of this relationship, let us analyze the "game" between the two, where each party chooses the strategy that best serves its interests, and look for equilibria.

The Game Setting

The basic conditions are the same as in game model 1.

Players: Player I is an individual who possesses private personal information.[6] Player II is an Internet company (for this example, let it be the company that owns Waze) whose Internet-based service the individual seeks to use.

Available **strategies:** Player I (the individual) has two possible strategies: to share their full information or to share only the minimal information[7] that is necessary for using the service.[8] Player II (the Internet company) also has two possible strategies: to keep the information to itself, or to trade it.[9]

The Game's Payoff Matrix

Let the general payoff matrix be:

	Information value for Player I		Information value for Player II	
	Player I shares full information	Player I shares minimal information	Player I shares full information	Player I shares minimal information
Player II maintains information confidentiality	(a)	(b)	(c)	(d)
	1.2	1	1.2	0.7
Player II sells the information	(e)	(f)	(g)	(h)
	-1	-0.5	0.9	0.2

Payoff matrix justification:

For Player I:

If Player II maintains the confidentiality of Player I's information, Player I will benefit the most from sharing full information with Player II: in our example, Player II (Waze) can give the driver Player I customized recommendations for stops along their route based on Player I's shopping preferences. Therefore, the information value is *1.2*. If Player I shares only the minimal information required, Player II will be able to provide exactly its declared service, and nothing more. Therefore, the information value for Player I in this case is *1*.If Player II violates its confidentiality commitment, Player I will suffer harm (e.g., the confidentiality breach will reveal who the driver has spoken to during the trip) at a value of *-1* if they shared their full information, or *-0.5* if they shared only the minimal information.

For Player II:

If Player II received full information from Player I, maintaining confidentiality allows it to fully realize its capabilities (in our example, Waze can offer extra services, such as customized recommendations for stops based on the driver's preferences), and therefore, the information value is *1.2* for it as well. If Player II received only the minimal information it needs to provide the service, the value of that information for Player II is *0.7*.

Violating Player I's confidentiality in case of possessing full information gives Player II a value of *0.9* (the value of selling the information). In case of partial information, the value of sales is only *0.2*.Importantly, when Player II is choosing a strategy, it cannot know whether Player I has given it full or partial information. Only Player I can know that.Based on this, we can calculate a more specific payoff matrix for each of the players. Let us mark Player I's payoffs as X_{ij}, with $i = 1$ meaning provision of full information by Player I, $i = 2$ meaning provision of partial information, $j = 1$ meaning maintaining of confidentiality by Player II, and $j = 2$ meaning violation of confidentiality. Similarly, let us mark Player II's payoffs as Y_{ij}. I am assuming Player II will always not only use the personal information it has received from Player I, but also sell it to maximize its profit.

The game payoffs will be as follows:

$X_{11} = (a) = 1.2$

$X_{12} = (a) + (e) = 1.2 + (-1) = 0.2$

[6]For the sake of this example, let Player I be a driver who wants to get from A to B.

[7] The minimal information that the Internet company needs in order to provide its declared service. In the case of Waze, it is the driver's phone number, the required destination, and Internet connection on the driver's phone.

[8] Reasons for choosing to share full information may include Player I's indifference to the ways their personal information may be used, or unawareness of the possibilities of improper use of their personal information. Choosing to share only the required minimum may be based on a belief that it will better serve the player's interests: e.g., if you do not disclose all your financial information, you may be able to get better loan terms.

[9] Choosing to maintain confidentiality usually stems from legal or normative obligation, while choosing to sell the information is usually motivated by the desire to make a profit from it.

$X_{21} = (b) = 1$
$X_{22} = (b) + (f) = 1 + (-0.5) = 0.5$

$Y_{11} = (c) = 1.2$
$Y_{12} = (c) + (g) = 1.2 + 0.9 = 2.1$
$Y_{21} = (d) = 0.7$
$Y_{22} = (d) + (h) = 0.7 + 0.2 = 0.9$

For convenience, let us display this payoff matrix in tabular form:

Player I's payoff matrix:

	Player I shares full information	Player I shares partial information
Player II maintains confidentiality	1.2	1
Player II breaches confidentiality	0.2	0.5

Player II's payoff matrix:

	Player I shares full information	Player I shares partial information
Player II maintains confidentiality	1.2	0.7
Player II breaches confidentiality	2.1	0.9

The game has a pure strategy Nash equilibrium. Player II has the dominant strategy: whatever the case, breaching Player I's confidentiality pays off. If Player I chooses the strategy of sharing full information, and Player II maintains its confidentiality, both will have a payoff of *1.2*. However, breaching confidentiality will increase Player II's payoff to *2.1*. Therefore, the best strategy for Player I will be to initially share only partial information, to secure a payoff of at least *0.5*. But even then, it still pays off for Player II to breach confidentiality, as their payoff will be *0.9* instead of *0.7*. Since neither player can do better than that, this is the Nash equilibrium of this game.This is an example of a one-time game of prisoner's dilemma, in which distrust between the individual and the Internet company leads to both of them not getting the optimal outcome they might have had if they had maintained general privacy. The cost of privacy violation is $1.2 - 0.5 = 0.7$ for Player I, and $1.2 - 0.9 = 0.3$ for Player II.We can assume there will also be a social cost for violating privacy in this game: $0.7 + 0.3 = 1$. This supports the argument that maintaining personal privacy serves society even more than it serves the individual.

Game Model 3: Confidant vs Internet Company

The personal information protection game scenario between a confidant entity[10] and an Internet company[11] is as follows:

In this game, each of the players possesses some private personal information of a given individual. Both received that information in exchange for their services. It does not matter whether the information is full or partial. Both players are committed to maintaining the individual's privacy, whether by law, by social norms, and/or by their own privacy policy. Both are sorely tempted to trade the personal information they possess, as it can bring them considerable profit; however, they may be fined if they breach their privacy obligations.Given this relationship, let us analyze the "game" between the two, where each party chooses the strategy that best serves its interests, and look for equilibrium points.

The Game Setting

The basic conditions are the same as in game models 1 and 2.

Players: Player I is a confidant, i.e., an entity in which individuals see a candidate for sharing their private personal information with;[12] Player II is an Internet company, e.g., Google.[13]

Available strategies: Player I (the confidant) has two possible strategies:to protect the individuals' privacy, or to trade their private information. Player II (the Internet company) also has two possible strategies: to protect the confidentiality of the information it possesses, or to trade it.[14]

The Game's Payoff Matrix

Let the general payoff matrix be:

	Information value for Player I		Information value for Player II	
	Player I maintains confidentiality	Player I breaches confidentiality	Player I maintains confidentiality	Player I breaches confidentiality
Player II maintains confidentiality	(a)	(b)	(c)	(d)
	1	-0.3	0.3	0.4
Player II breaches confidentiality	(e)	(f)	(g)	(h)
	0.2	0.9	-0.2	1.5

Payoff matrix justification:

For Player I:

If both Player I and Player II maintain the confidentiality of the personal information in their possession, Player I has no additional gain beyond the gain it already has from being a confidant; therefore, the value of the information for it is *1*. If Player I maintains confidentiality, but Player II does not, Player I has an additional gain of *0.2* from obtaining new information it did not initially have. If Player I does not maintain confidentiality, but Player II does, Player I profits from selling the information in its possession, but may be fined for privacy violations,[15] which makes its total payoff negative – *-0.3*. If both players breach confidentiality, Player I gains more from obtaining new information it did not initially have, which outweighs any potential fines and leaves it with a total payoff of *0.9*.

For Player II:

If both Player I and Player II maintain confidentiality, Player II gains only from the information it has in its possession; however, that gain should be cut off against the costs of the service it provides to the user "for free", which makes its total payoff *0.3*. If Player II maintains confidentiality, but Player I does not, Player II gains from obtaining new information from Player I, and is not subject to any fines itself, meaning an additional gain of *0.4*. If Player II does not maintain confidentiality, but Player I does, Player II profits from selling

[10] An entity that serves as a confidant to an individual.

[11] E.g., Google.

[12] For the sake of this example, let Player I be a health insurance company whose representatives search medical information about individuals online.

[13] The search engine where Player I is looking for medical information.

[14] Choosing to maintain confidentiality usually stems from legal or normative obligation, while choosing to sell the information is usually motivated by the desire to make a profit of it.

[15] If it is bound by privacy protection laws. It is also at risk of being reported by Player II.

the information in its possession. It may be fined at a value of *0.2* for privacy violations,[16] but the fine is outweighed by the profit it gains from selling the information. If both players breach confidentiality, Player II has additional gain from obtaining new information it did not previously have, and is at lesser risk of being fined: when an individual's confidentiality is breached by more than one entity, it is harder to find who is guilty; both players can play a "blame game" and eventually get away with virtually no punishment. Therefore, in this case, Player II's payoff is *1.5*.

Thus, if both players breach individuals' confidentiality and simultaneously deny it, Player II gains the mostbecause it possesses more personal information that it can trade, as we saw in the discussion of surveillance capitalism.

Based on this, we can calculate a more specific payoff matrix for each of the players. Let us mark Player I's payoffs as X_{ij}, with $i = 1$ meaning maintaining of confidentiality and $i = 2$ meaning violation of confidentiality by Player I, and with $j = 1$ meaning maintaining of confidentiality and $j = 2$ meaning violation of confidentiality by Player II. Similarly, let us mark Player II's payoffs as Y_{ij}.

The game payoffs will be as follows:

$X_{11} = (a) = 1$
$X_{12} = (a) + (e) = 1 + 0.2 = 1.2$
$X_{21} = (b) = -0.3$
$X_{22} = (b) + (f) = -0.3 + 0.9 = 0.6$

$Y_{11} = (c) = 0.3$
$Y_{12} = (c) + (g) = 0.3 – 0.2 = 0.1$
$Y_{21} = (d) = 0.4$
$Y_{22} = (d) + (h) = 0.4 + 1.5 = 1.9$

For convenience, let us display this payoff matrix in tabular form:

Player I's payoff matrix:

	Player I maintains confidentiality	Player I breaches confidentiality
Player II maintains confidentiality	1	-0.3
Player II breaches confidentiality	1.2	0.6

Player II's payoff matrix:

	Player I maintains confidentiality	Player I breaches confidentiality
Player II maintains confidentiality	0.3	0.4
Player II breaches confidentiality	0.1	1.9

The game has two possible equilibria. In the case of the equilibrium where both players choose to maintain confidentiality, neither of them individually can benefit from changing their strategy. The same goes for the other equilibrium – both players choosing to breach confidentiality. According to David Lewis, in situations like this, we see a shift from a zero-sum game to a coordination game [8].

This can be achieved by switching from a game of pure strategies to a game of mixed strategies, as follows [9]:

		1 - p = 0.12	p = 0.88
		Player I maintains confidentiality	Player I breaches confidentiality
1 – q = 0.74	Player II maintains confidentiality	1, 0.3	-0.3, 0.4
q = 0.26	Player II breaches confidentiality	1.2, 0.1	0.6, 1.9

Let $0 \leq p \leq 1$ be the probability of Player I choosing to breach confidentiality, and $1 – p$ the probability of Player I choosing to maintain confidentiality. Respectively, let $0 \leq q \leq 1$ be the probability of Player II choosing to breach confidentiality, and $1 – q$ the probability of Player II choosing to maintain confidentiality. p and q can be calculated using the following formulae:

$p \cdot (-0.3 + 0.6) = (1 – p) \cdot 1 + (1 – p) \cdot 1.2 \rightarrow p \cdot 0.3 = 2.2 – p \cdot 2.2 \rightarrow p = 0.88, (1 – p) = 0.12$
$q \cdot (0.1 + 1.9) = (1 – q) \cdot 0.3 + (1 – q) \cdot 0.4 \rightarrow q \cdot 2 = 0.7 – q \cdot 0.7 \rightarrow q = 0.26, (1 – q) = 0.74$

Now, we can calculate the expected utility for both players using this formula:

$$\sum_{i=1}^{2}\sum_{j=1}^{2} Aij$$

The expected utility for Player I:

$\sum_{i=1}^{2}\sum_{j=1}^{2} Aij = 0.88 \cdot 0.26 \cdot (-0.3 + 0.6) + 0.12 \cdot 0.74 \cdot (1 + 1.2) = 0.27$

The expected utility for Player II:

$\sum_{i=1}^{2}\sum_{j=1}^{2} Aij = 0.88 \cdot 0.26 \cdot (0.4 + 1.9) + 0.12 \cdot 0.74 \cdot (0.3 + 0.1) = 0.56$

Both players' utility in a mixed strategy Nash equilibrium is smaller compared to what they will get if they stick to their pure strategy. **Player I** gets a utility of *1* if both players maintain the confidentiality of the information, which means a loss of *0.73* in a switch to mixed strategy. **Player II** gets a utility of *1.9*if both players breach confidentiality, which means a loss of *1.34*in mixed strategy. Lewis explains that the reason players choose to play a coordination game is their expectation that this is the behavior expected of them [8]. In our example, the players will violate confidentiality because they believe that "this is what everyone does" and that individuals are not actually expecting anyone besides themselves to protect the confidentiality of their information.

Conclusions

In the first two game models discussed here, Player II has a dominant strategy that supports the violation of the privacy of Player I (an individual). This accurately reflects the current state of events in the field of Internet privacy. To improve this situation, either and/or all of the following should happen: one possible solution is the more severe fining of confidants and Internet companies who violate personal privacy; this is the purpose of the GDPR. However, this is not enough; the paradigm of personal privacy that is founded on consent and control [10] should be replaced by a new one that would pass the responsibility for privacy protection from the individuals, who are expected to give consent and have control over their personal information, to the Internet companies and confidants,

[16] E.g., if it violates the GDPR.

who should be held responsible and liable for fair and proper use of the said information. is putting a price tag on personal information[11] and imposing the costs on Internet companies to restrain their uncontrollable appetite for using personal information as a free resource they can profit from.The third model discussed here should be harder to manage financially because Internet companies, which are practically monopolies, have the most to gain from violating our personal privacy. Probably the best way to handle this situation is by stricter regulation and social norms.

REFERENCES

1. Oppenheim, Yair , Personal Privacy in the Age of the Internet. Spines, 23 Sep 2024, 122-135. For a discussion of the cracks in the current paradigm of personal privacy
2. Lisa Rajbhandari and Einar Arthur Snekkenes, "Using Game Theory to Analyze Risk to Privacy: An Initial Insight", presented at IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, 2010, 42.
3. Ibid., 43.
4. Michael Maschler, Eilon Solan and Shmuel Zamir, *Game Theory* (New York: Cambridge University Press, 2013), 97.
5. Ibid., 105.
6. Robert Aumann, Yair Tauman and Shmuel Zamir, *Torat ha-miskhakim – Yekhidot 1, 2,* 3 [Game *Theory – Units 1, 2 & 3*] (in Hebrew) (Tel Aviv: Everyman's University, 1981), 19.
7. Oppenheim, Yair, Personal Privacy in the Age of the Internet. Spines, 23 Sep 2024, 167-190.
8. David Lewis, *Convention: A Philosophical Study* (Cambridge: Harvard University Press, 1969), 5-51.
9. Robert Aumann, Yair Tauman and Shmuel Zamir, *Torat ha-miskhakim – Yekhidot 1, 2,* 3 [Game *Theory – Units 1, 2 & 3*] (in Hebrew) (Tel Aviv: Everyman's University, 1981), 134-139.
10. Oppenheim, Yair , Personal Privacy in the Age of the Internet. Spines, 23 Sep 2024, 266 - 288.
11. Ibid.,See the proposition to tax Internet companies based on the amount (in kilobytes) of personal privacy information they use.

****