Field Research beroepsethiek

October 25, 2017

Alexander Plet (500756442)

Sjors Gielen (500765899)

Inhoudsopgave

Samenvatting

Tijdens dit onderzoek hebben wij aandacht besteed aan het omgaan van gebruikersdata binnen de (game)industrie. De data dat wordt opgeslagen heeft een bepaalde gevoeligheid dat verschilt per inhoud. In het vooronderzoek hebben wij onderzoek gedaan over het beroeps ethiek in de IT wereld door ons te richten op de hoofdvraag. De hoofdvraag luidt: Hoe moeten (game)bedrijven omgaan met de gebruiker/speler data die zij opnemen. Deze vraag hebben wij beantwoord door informatie online erover te vinden waarvan de bron in dit document naar wordt verwezen. Bedrijven die data van hun gebruikers opslaan hebben meerdere levels wanneer het aankomt op de gevoeligheid van de gegevens. Je zou het kunnen classificeren in drie delen. Laag, middel en hoog. Dit representeert de gevoeligheid van de toegewezen data. Bij laag zou er gedacht kunnen worden aan cookies van een website dat bezocht is. Aan hoog kan er gedacht worden aan betalingsgegevens. Met genoeg gegevens bij de hand is het mogelijk om anonieme data die een link met elkaar hebben te koppelen zodat er een patroon in te zien is en uiteindelijk een individu uit te halen in het systeem. Dit kan gedaan worden door iedereen en daar is geen toestemming voor nodig. Wanneer de gegevens voor iemand staan met de rechten om het te mogen bekijken is dit mogelijk. Anders niet.

Verder zijn wij op pad geweest om een fieldresearch te doen over het onderwerp. Wij hebben ieder onze respectieve geïnterviewde individu benaderd over dit onderwerp. Hieruit is gebleken dat de informatie van het vooronderzoek goed samenhangt met wat er aan ons verteld is tijdens de interviews. Ook hebben wij uit eigen initiatief een google questionnaire aangemaakt om te zien wat onze vrienden, familie en medemens denkt over de manier waarop data van de gebruikers gebruikt wordt binnen een bedrijf.

Tot slot zijn we erachter gekomen hoe er gedacht wordt over hoe (game)bedrijven om zouden moeten gaan met de data dat binnenkomt van hun gebruikers. Dit is immers dat de data wat binnenkomt dat nuttig is voor het bedrijf opgeslagen wordt door middel van een versleuteling zodat niet iedereen bij deze informatie terecht kan over de gebruikers. De rest van de data dat binnenkomt kan verworpen worden aangezien het niets toevoegt om te behouden. Aldus nutteloze informatie over de klant kan liever niet opgeslagen worden.

1 Inleiding

In dit field research willen wij ons een beetje gaan verdiepen in de omgang met data, hierbij willen wij ons vooral focussen op gamebedrijven. Over het algemeen is het wel vrij lastig om een dialoog te beginnen over gebruikersdata met gamebedrijven dus hebben wij IT specialisten geïnterviewd om een beeld te scheppen over algemene bedrijven en een questionnaire uitgevoerd om een beeld te scheppen van de klantenbasis.

Op een globale basis is het doel om duidelijkheid te scheppen vanuit een ethisch perspectief hoe een gamebedrijf om zou moeten gaan met eventuele data van de klantenbasis dat zij opnemen en/of behandelen. Hiervoor is natuurlijk belangrijk om te weten hoe de klantenbasis zich opstelt ten opzichte van data opslag en gebruik.

Wat ondere andere een zeer groot belang heeft is hoe gevoelig data is en wat het nou zo gevoelig maakt. Is alleen een naam gevoelig of is alleen een land gevoelig? Wat als we de twee samenvoegen, is dat dan nog gevoeliger? Of verandert dit niet?

2. Belangrijkste Hypothesen uit het vooronderzoek

2.1 Wat voor type data kan een game developer opnemen?

Van de speler data kan ontzettend veel worden opgenomen. Bij een online spel wordt verwacht dat de gebruikers IP, Packet loss rate en internet connection speed bij kunnen worden gehouden.
Verder wordt verwacht dat invoer die de speler verricht ook wordt opgenomen tot op een zeker niveau. Het resultaat(spelletje gewonnen of niet), de duratie van een spel en de duratie van een sessie worden bijgehouden. Als een spel een text-based chat systeem gebruikt wordt er verwacht dat hier een ook een log van wordt bijgehouden. Buiten deze generieke verwachten gaan wij er haast vanuit dat wij onderdelen hebben gemist op een game-by-game basis. Welke deze precies zijn kan hier dus een groot punt van interesse zijn.

2.2 Wat maakt bepaalde data gevoeliger dan de rest?; Per classificatie, hoe gevoelig is de data?

Hier wordt verwacht dat elke desde dichterbij de classificatie van data ligt bij de persoon waar het van is gekomen desde gevoeliger het is. Bijvoorbeeld de invoer van een gebruiker in een game is minder gevoelig dan de gebruikers IP address.

2.3 Hoe worden lijsten geanonimiseerd?; en is dat wel goed genoeg?

Data met een hoge gevoeligheids classificatie worden uit de lijsten verwijderd. Bijvoorbeeld namen en IP adressen. Maar mogelijk ook chat logs om te voorkomen dat pattern analyse wordt gebruikt op gebruikers text patronen.

2.4 Hoe makkelijk is het om een geanonimiseerde lijst weer niet anonym te maken?

Verwacht hier is dat voor elke lijst waar al een vergelijkbare lijst bestaat het steeds makkelijker wordt. Bijvoorbeeld als er een lijst van gebruikersnamen en wachtwoorden bekend wordt gemaakt. Als er een gebruikersnaam en wachtwoord combinatie op site 1 en op site 2 bestaan dan is het zeer waarschijnlijk dat dit dezelfde persoon zal zijn.

2.5 Hoe willen gamers dat er word omgegaan met hun gebruikers data?(per classificatie)

De normale gebruikers maken vaker meer ophef over hun data dat rond verdeelt. Terwijl het bij gamers minder uitmaakt zolang er geen persoonlijke data wordt weergegeven.

2.6 Hoe moeten gamebedrijven omgaan met de spelers data die zij opnemen?

Hier zijn twee onderdelen belangrijk hoe gamers(en andere gebruikers) zich voelen over de classificaties en of de data well of niet word geanonimiseerd. De methode van anonimisering maakt waarschijnlijk ook uit. Maar zijn ook bepaalde stukken data waarvoor het waarschijnlijk beter is als het bedrijf ze wel publiek maakt. Bijvoorbeeld hoeveel gebruikers er huidig actief zijn in een matchmaking queue.

3 Resultaten van het field research

3.1 Interviews

Gebleken uit de interview met Rega Schardijn en Joe Zack is bekend dat er bij beide bedrijven ongeveer dezelfde data binnenkomt van de klanten die zij hebben. Hierbij kan gedacht worden aan NAW(Naam, Adres en Woonplaats), telefoonnummer, e-mailadres, transactionele gegevens en dergelijke. De binnenkomende data is onderverdeeld in verschillende levels van kwetsbaarheid. Zo is bijvoorbeeld de naam van de klant minder gevoelig dan de bankgegevens van de klant. En dat een klant een specifieke item heeft besteld ergens nog minder gevoelig. Maar zodra je gegevens kunt linken aan elkaar begint het gevaarlijk te worden, want dan blijkt het dat de data toch niet zo anoniem is dan wat je verwacht. Hier heb je geen toestemming voor nodig om zelf een link te leggen tussen de data. Natuurlijk zijn de gegevens beveiligd onder meerdere lagen binnen de beveiligde omgeving tussen de klant en de virtuele werkomgeving. De werknemer heeft door middel van credentials toegang tot de virtuele werkomgeving waarin de werknemer klantgegevens benaderd. Doordat de werknemer geen toegang heeft tot alle gegevens is het de taak van de systeembeheerders om dagelijks de gegevens vanuit de klant hun eigen werknemers omgeving te monitoren en te beheren.

Joe Zack liet blijken dat niet alle data dat binnenkomt van de gebruiker nodig is. Het resterende data is niet noodzakelijk om op te slaan. Ook is het mogelijk door encryptie (versleutelen) de data beveiligen. Dit is om te voorkomen dat onbevoegden de data kunnen bekijken en kunnen lekken.

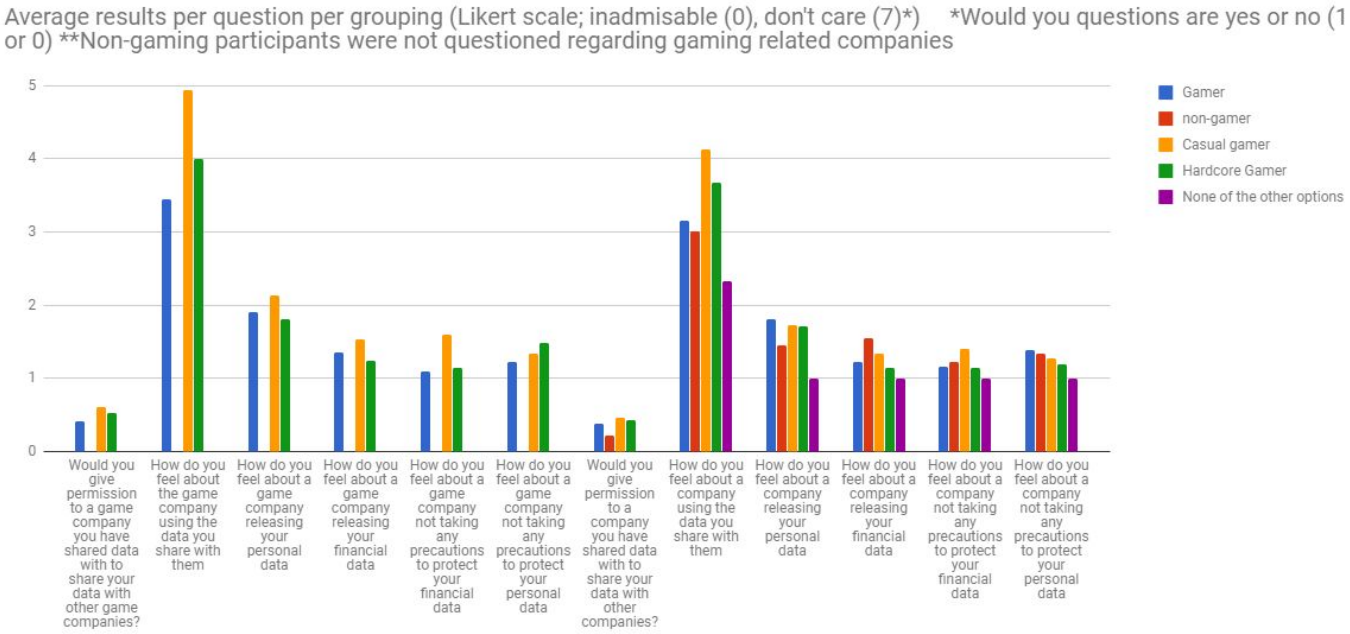
Data van de klant wordt opgeslagen in de systemen van de bedrijven. De bedrijven hebben gegarandeerd de data dat is opgegeven door de klant zelf. Hoewel de klanten weten dat de bedrijven hun data hebben weten ze niet wat ermee gedaan wordt. Bij sommige bedrijven kun je aanvragen wat er gedaan wordt met de klantdata, zoals bij Google. Over het algemeen willen klanten niet dat hun gegevens publiekelijk te zien zijn. Dit telt vooral met persoonlijke gegevens. Alhoewel er ook gegevens zijn die je niet kunt koppelen aan een individu als er maar een deel ervan vrijgegeven wordt. Denk hierbij maar aan het aantal uren dat een gebruiker online is gemiddeld.

Indien een bedrijf ooit gehacken wordt is er een bepaald patroon die de bedrijf in werking stelt. De P, D en R. Preventie, Detectie en Reactie.

Met preventie wordt de firewall bedoelt om aanvallers buiten te houden. Er word veel meer gefocust op de D en R zaken omdat er altijd nieuwe manieren worden uitgevonden om iets/iemand te hacken. Detectie is wanneer er gemerkt wordt dat iets of iemand in het systeem zit zonder bevoegd baarheid. Vaak wordt er eerst gekeken naar wat voor schade er al gedaan is en word er een plan toegepast over hoe het bedrijf het gaat aanpakken. Door Reactie toe te passen is er een passende aanpak op de detectie.

Tot slot is het mogelijk voor de klant om data dat in het systeem van het bedrijf staat van henzelf aan te vragen. Het bedrijf zal dan geven wat ze realiseren dat ze de klant kunnen geven. Aangezien het onzeker is om alles te geven wat er bekend is bij hen.

3.2 Questionnaire



Uit de resultaten van de questionnaire zien we dat er over het algemeen geen grote verschillen zijn in de gemaakte groeperingen.

Wat hier echter wel interessant uit is dat een hoog percentage mensen vindt dat het delen van persoonlijke informatie tussen bedrijven een groot probleem is terwijl het erg veel gebeurt(Interview Joe Zack).

Ook een interessante conclusie hieruit is dat over het algemeen gamers het ietsjes minder erg vinden wat er met hun data gebeurt. Een effect dat zeker wordt versterkt bij intern gebruik van een gamebedrijf. Wij vermoeden dat dit vooral komt door een gebrek aan kennis bij de consumenten over data binnen in IT sector als dit wordt vergeleken met de interviews.

4 Conclusie

Uit het vooronderzoek en het fieldresearch blijkt dat de informatie dat verzameld is gedurende het vooronderzoek overeenkomt met hoe er gedacht wordt over het onderwerp door ons, de geïnterviewden en de mensen die onze google questionnaire hebben beantwoord. Dit is te zien door de antwoorden te vergelijken. De gebruikers willen niet dat bedrijven hun data publiek maken. Terwijl de gamer gebruikers het iets minder erg vinden zolang het maar niet gaat over hun persoonlijke data wat te achterhalen is. Wat de gebruikers niet weten is dat een bedrijf meerdere vormen van data opslaat van de gebruiker waar de gebruiker zelf niets of weinig van af weet. Denk hierbij maar aan cookies van websites. Omdat een bedrijf veel data binnen krijgt van de gebruiker is het mogelijk om de data te classificeren. Dit heeft te maken met de privacygevoeligheid. Hoe gevoeliger de data hoe meer de data versleuteld zou moeten zijn. Met veel data is het mogelijk om de anonieme data te vergelijken met elkaar om een patroon te vinden. Dit is alleen mogelijk voor de mensen die bevoegd zijn in dat gebied, zoals een systeem/database beheerder die dagelijkse de klant hun eigen werknemers omgeving beheerd.

Bronnenlijst

1. Wood, Richard T A ; Griffiths, Mark D ; Eatough, Virginia
   Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society, October 2004, Vol.7(5), pp.511-8
2. IBM (z.d.). What is Big Data?. Geraadpleegd op 3 oktober 2017, van https://www.ibm.com/analytics/us/en/big-data/

Appendix

Interview vragen:

1. Wat voor data ontvangen jullie?
2. Hoe gaan jullie om met het ontvangen van data?
3. Weet de klant welke data er van hen wordt opgeslagen?
    a. Ja →
        i. Hoe word dit gecommuniceerd naar de klant?
        ii. Welke data van hen word er opgeslagen?
    b. Nee →
        i. Waarom weet de klant hier niet over?
4. Weet de klant waar hun data naartoe gaat?
    a. Ja →
        i. Hoe word dit gecommuniceerd naar de klant?
    b. Nee →
        i. Waarom weet de klant hier niet over?
5. Wat wordt er intern met de data van klanten gedaan?
6. Maken jullie data van klanten publiek?
    a. Ja →
        i. Welke data wordt publiek gemaakt?
        ii. In welke vorm word deze data publiek gemaakt?
    b. Nee →
        i. Waarom wordt er geen klanten data publiek gemaakt?
        ii. (eventueel) Als de klanten data wordt geanonimiseerd, zouden jullie de data dan wel (deels) publiek maken?
7. Hoe wordt de gevoelige data afgezonderd van de rest?
8. Hoe zit het met de beveiliging van de klant wanneer jullie systeem risico loopt?
9. Kan de klant zelf navragen wat er opgeslagen wordt aan data van hen?
    a. Waarom wel/niet?

Interview Rega Schardijn

Wat voor data ontvangen jullie?

-Wij hebben verschillende soorten klanten die op dit moment in verschillende projecten zitten zoals in de retail, leden organisatie en off-shore.

Ik implementeer voor ERP systemen (Enterprise resource planning systemen) en klantendata voor Erp B.I (business intelligence). Ik begrijp hoe ze hun data willen automatiseren voor hulp met het genereren van informatie uit ERP systemen. De data die wij binnenkrijgen zijn: stand gegevens, transactionele data (retour data en transacties).

Wat maakt bepaalde data gevoeliger dan de rest?; Per classificatie, hoe gevoelig is de data?

Het gebruik van klantdata binnen onze systemen maakt de data gevoelig. De datatypes hiervan zijn privacygevoelig. Dit zijn gegevens zoals eerder al is gezegd; de stand gegevens en transactionele data(retourdata en de transacties).

Hoe worden lijsten geanonimiseerd?(en is dat wel goed genoeg?)

Als werknemer ben je verantwoordelijk voor het gebruik maken, verwerken en delen van de klantdata. Deze activiteiten vinden plaats in een beveiligde omgeving tussen de klant en de virtuele werkomgeving. Door middel van AAD -Azure Active Directory kun je met je eigen credentials vanuit de werkomgeving de klantomgeving benaderen.
Zelf vind ik het genoeg omdat ik als werknemer zelf niet bij alle data kan binnentreden.
De AAD wordt dagelijks gemonitord en beheerd door de systeembeheerders vanuit de klant hun eigen werknemers omgeving.

Hoe makkelijk is het om een geanonimiseerde lijst weer niet anonym te maken?

Het is te achterhalen waar de informatie vandaan komt, wanneer en door wie zonder eerst na te vragen of je het mag inzien. Enkelingen kunnen dit als je de rechten ervoor hebt.

Hoe willen klanten dat er word omgegaan met hun gebruikers data?(per classificatie)

Dagelijks heb ik te maken met een klant die zijn contract beëindigd met bedrijven. Daarin is alle informatie te zien over de transacties en de NAW (naam, adres, woonplaats) gegevens. De gegevens worden kort bewaard indien de klant wilt terugkomen zodat de gegevens niet allemaal verwijderd zijn van het systeem wanneer dat het geval is.

Hoe moeten bedrijven omgaan met de klanten data die zij opnemen?

Wij als consultants moet met de klant een overeenkomst aangaan met betrekking tot het gebruikmaken van de klantgegevens gedurende de implementatie trajecten. Deze overeenkomst heeft betrekking tot het bewerken en beheren van deze data.

Interview Joe Zack

Could you please tell me briefly who you are and what experience in IT you have?

I'm Joe Zack, software developer for the last 15 years, worked in ecommerce, content management tools, social media, working security and I also do a software engineering podcast (Coding blocks).

What kind of data do you guys receive?

Depending on the kind of company you work on you can receive, personally identifiable information; which is anything that could uniquely identify an individual person, so for example an e-mail address, phone number or last name and first name. Different companies can have different qualifications to what would count. Some may count just an address, or some may count a first name, last name and zipcode. Other kinds of information such as billing information; credit cards, social security numbers(also PII), chat logs.

Some of these could be irrelevant or could have legal implications.

In allot of cases they store a large bunch of analytics. For example by storing your browser fingerprint.

What are the classifications you generally give to data?

Depending on the maturity and size you'll see different classifications such as red or critical which would often hold PII, such as social security number or credit card information. Orange might be things like city, state and zip, but could even contain product information depending on if it is tied to PII. For example if the president could be identified to have purchased a racy book such as fifty shades of grey could be the news story of the day, and that leaves us with green. Stuff we don't really care about. Time stamps or large geographical locations which are hard to tie back to a person.

What you can kinda see is that the mix matching becomes important, as you could use two green pieces of information like country and email to make the search much smaller; phone number and zip-code.

There have been several instances where people tried to do some anonymizing data but being able to cross correlate that data to identify people anyway.

How would you deal with client data in general?

Ideally, just not store it at all. If you don't need to store then simply don't. For example chat logs. Next best case is to hash or encrypt it, but then you can't easily retrieve the data or query over the data.

If you do have PII stored with a way to access it another good thing to do is to throttle the customer service agent. For example the customer service agent can only look at x amount of records without triggering any kinds of alarms. On top of that they often use the security questions to ensure that the customer service agent can only access the data if they have the answers to the security questions, otherwise there would be some legal ramifications as the customer service agent could otherwise lookup the data of anyone whom has ever used that store.

Then there is also a paperwork solution where you make a deal with the company and or any third party's so that if they break that deal you can hold them financially liable.

Does the client know what data is being stored of theirs?

It's allot better than it used to be due to the EU and allot of mobile policies. But ultimately allot of data about you as customer is generated of the data you do have. So it's hard to draw the line between what the company can know from you can what you should know they know.

But even then it's an overwhelming amount of information to convey too the customers. Let alone ensure that is on a computer science literate method. For example try asking your grandmother what a cookie is.

Does the client know what happens with their data, where it is being stored etc?

Most of the time the customer doesn't. With some companies you can request it but it's really hard to say even then. Google could claim to ensure but it's really hard for them to even say as if they are using a third party and that third party is using third parties you get this crazy dependency chain. So in the end the communication burden is far too high and changes all the time.

What happens internally with client data?

Ideally storing as little as possible, encrypting the stuff that you do need to, or hashing it. Allot of the times companies will have policies about data in motion and data in rest. Which refers either encrypting the data between servers and services and on disc. Still not great. Some more advanced databases will have more fine-grain settings; have different rows encrypted differently so it's not the whole database, but each particular row or column is encrypted with different keys. Which would make it really difficult to crack. Which would only make it more difficult for any potential attacker. But ultimately there is no such thing as perfect security.

Is there any type of client data that you would make purposefully public?

Yea there are a couple of examples where things are public and or semi-public for example utility companies where your phone number is your username and if there is some crappy password reset processor you can actually figure out where those phone numbers have accounts, so if you are a bounty hunter you could pop in their phone numbers to see if they have an account there. Then if the error message is bad enough(or insecure enough) you could figure out in what kinda area of the world they may be living in, combine that with some phone calls and social engineering and you could figure allot out.

But allot of times information that is public you may not even realize is customer information. Sometimes for example if your kid has a baseball team, those teams would have a website where they have the kids first and last name, that is PII. It may not be very meaningful but too specific people, like the bounty hunter who is trying to find someone who is trying to skip bail, they might now that person has a kid, whose name is now showing up on some baseball site. With that track down the location of that team and know more information about the person they are trying to track down.

What often happens within companies though is that a third party service like dropbox is used to send client data between two people. For example if one person needs to send over a big excel file of clients that need a refund to the person who can actually perform that action, but the e-mail client provided by the company doesn't let you send over files of that size.

Is there any type of segregation in data and is that based on the classifications set out before(red, orange, green).

We seen some stuff like that where things are on separate table's or separate hardware. But I see it more often now to just secure everything. Using something like Oauth.

What happens to any client data if a risk/hack is detected?

There is the P the D and the R. Prevention, Detection and Reaction.

Prevention is the firewall, not storing data and anything you can do to keep attackers out.

Most of the focus is on the D and the R. Because new techniques and new vulnerabilities happen all the time. Unfortunately even though you know something bad has happened doesn't mean you know what to do about it. For example if a ex-workers account is suddenly logged into after the worker being fired for 3 years. Then thats a sign that something really bad has happened. Say you have some security software that noticed that doesn't mean you know what to do about it. Most of the times you can't even turn that server off and even if you could there is often isn't even a legal reason to do so. You may be saving your customers data by turning it off now but they could have already gotten it 3 months ago. Most of the time there isn't even any kind of repercussion for leaving things running. So most of the time some problem is detected people will just let it roll while they investigate, until they know exactly what happened, what they

took, how they did it, who got it and what needs to be done to prevent it. You can imagine that if you just turn the server off you tip your hat too the hacker that you are on to them. Which is not necessarily a good thing. So it may be safer bet to make for the customer but not necessarily for the company.

If you can focus on the Detection very well. The problem then becomes that you get a huge amount of Detections. So the real challenge then becomes to weed through the noise to find the really important things.

Is it possible for the client to request the company what type of data is being stored from them?

Some companies do that, google does it somewhat, Riot does it a little as well.

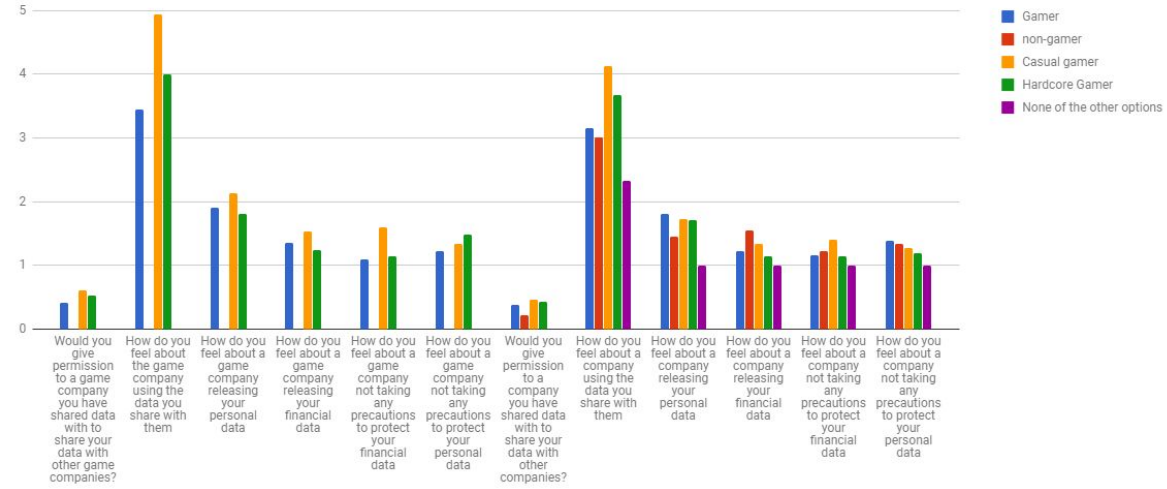
But for the most part it is what they want to give you, what they can give you and what they realize they can give you, there is no real way to be sure of them giving you everything. Even if the EU came out tommorow that every company has to have it be possible that if you fill in your e-mail address that they output all your data. As even then there is no real way to know if they give you all the data they have. Anything missing could just be claimed to have been purged. So proving that they aren't giving you everything seems nearly impossible.

Then on top of that should they give you the data they obtain through cross pollination? Say RiotGames has a deal with Domino's pizza. If you request the data from Riot, is Riot required to give you the data they have on you from domino's(Like your favorite pizza's)?

Then how do you even get everything from a user. First you look at the user table, address table, logging table, every notification we ever sent you.

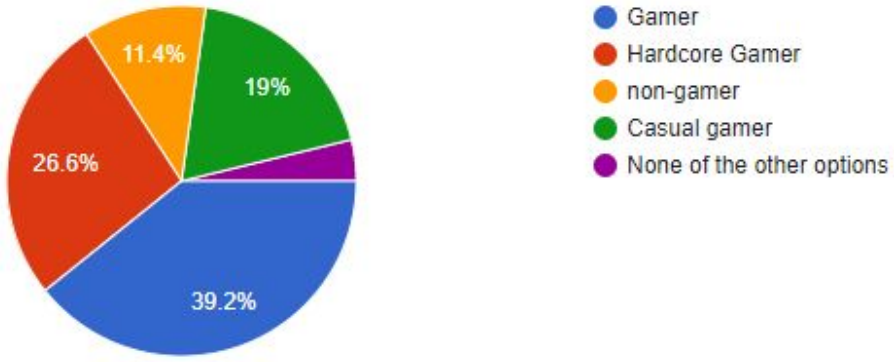
Questionnaire results

Average results per question per grouping (Likert scale; inadmisable (0), don't care (7)*) *Would you questions are yes or no (1 or 0) **Non-gaming participants were not questioned regarding gaming related companies



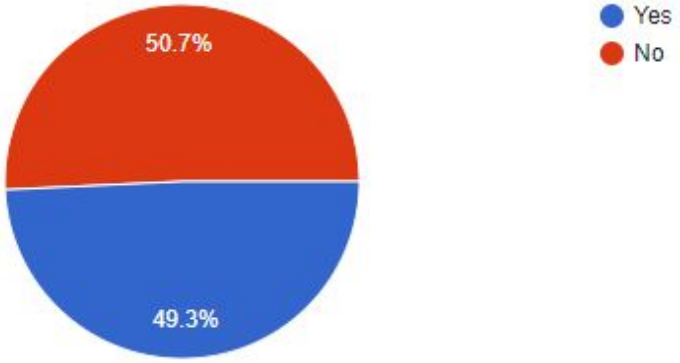
Which of the following categories do you match with the most

79 responses



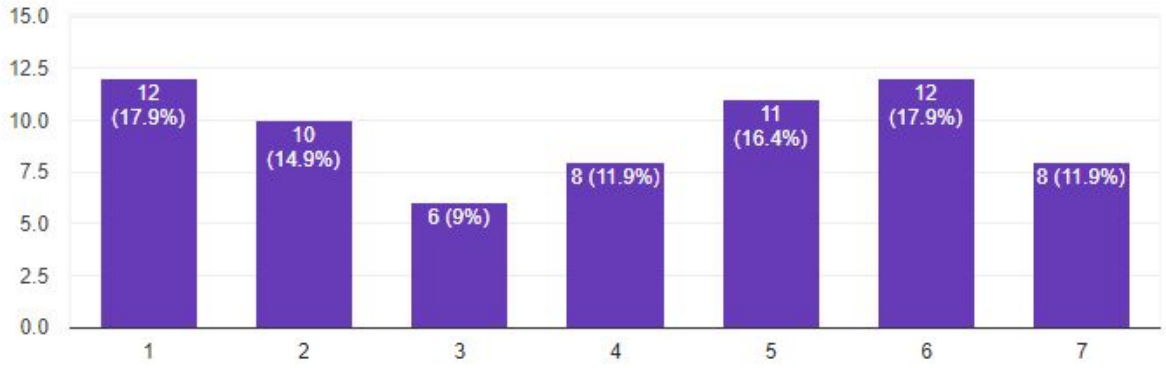
Would you give permission to a game company you have shared data with to share your data with other game companies?

67 responses



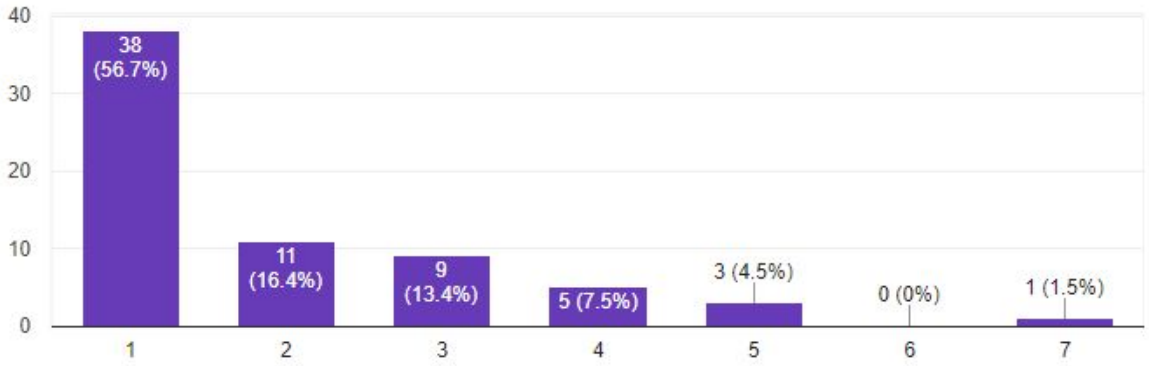
How do you feel about the game company using the data you share with them

67 responses



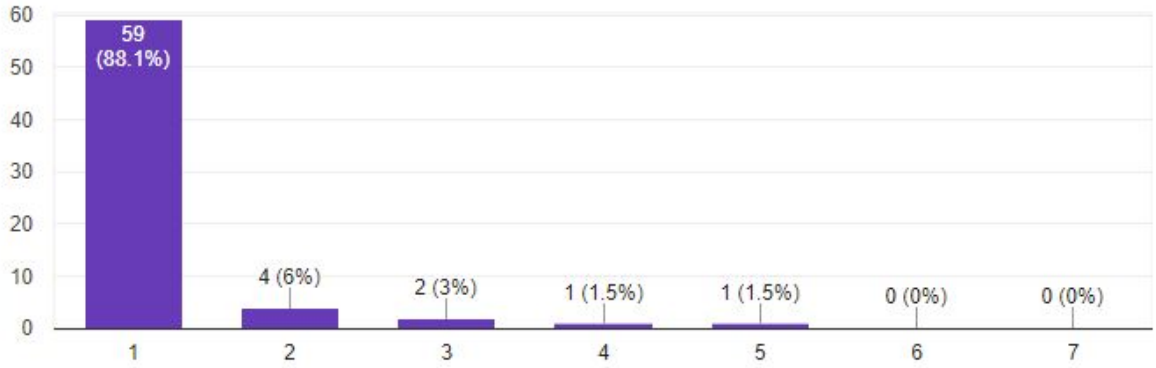
How do you feel about a game company releasing your personal data

67 responses



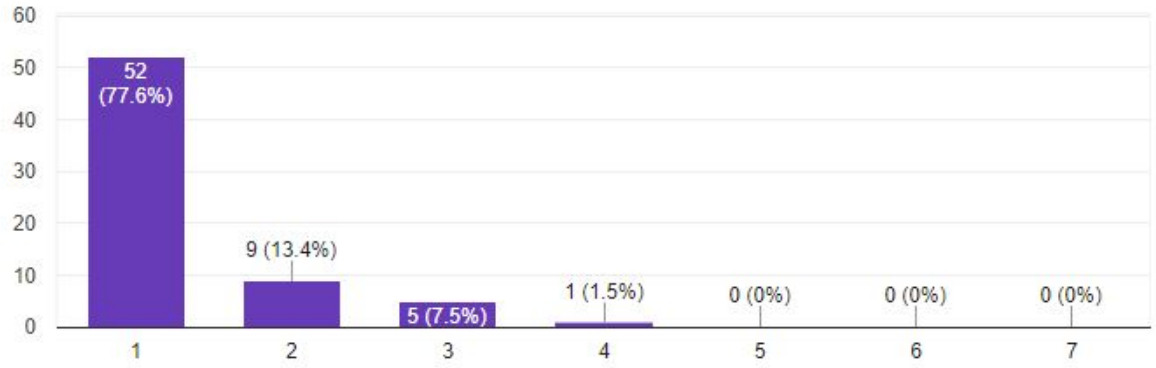
How do you feel about a game company not taking any precautions to protect your financial data

67 responses



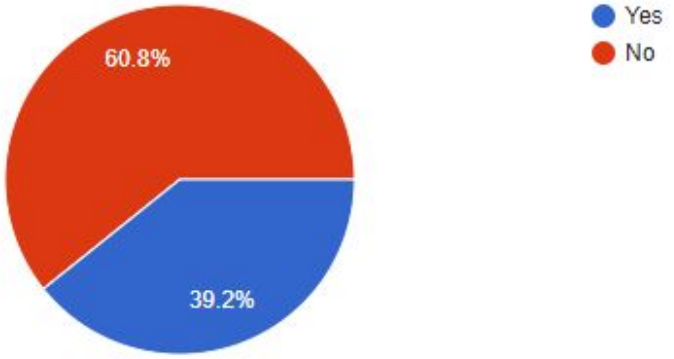
How do you feel about a game company not taking any precautions to protect your personal data

67 responses



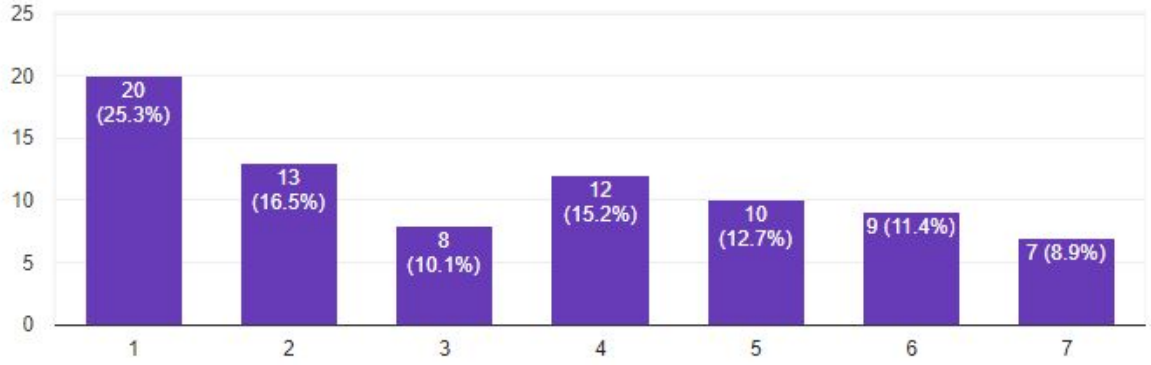
Would you give permission to a company you have shared data with to share your data with other companies?

79 responses



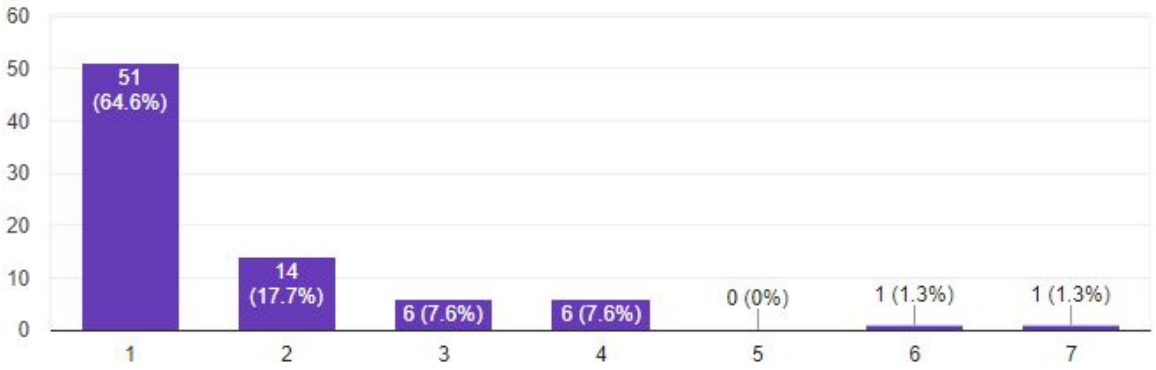
How do you feel about a company using the data you share with them

79 responses



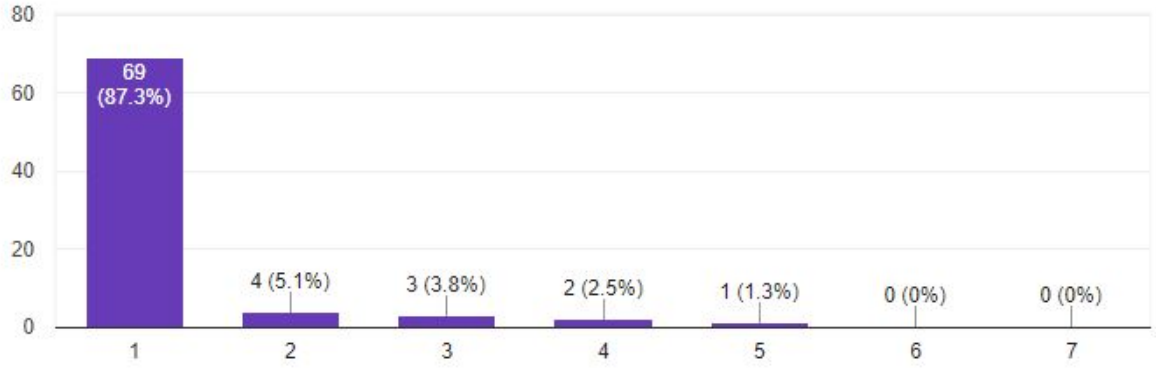
How do you feel about a company releasing your personal data

79 responses



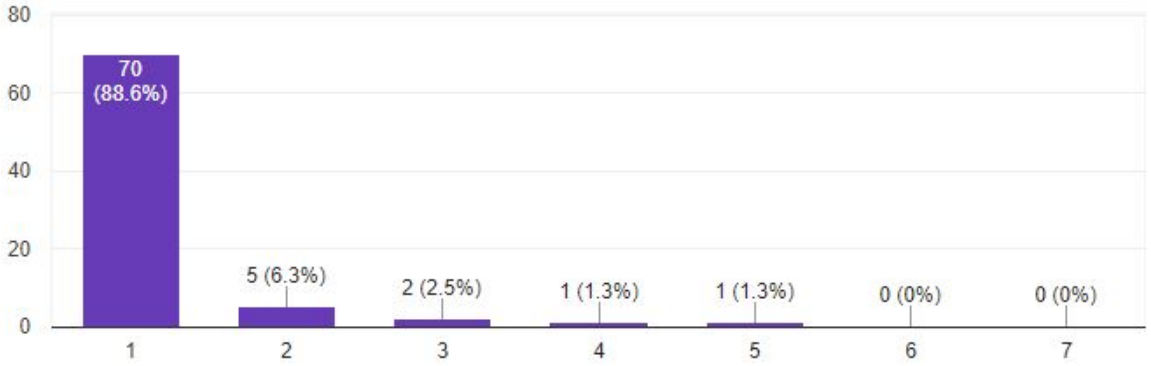
How do you feel about a company releasing your financial data

79 responses



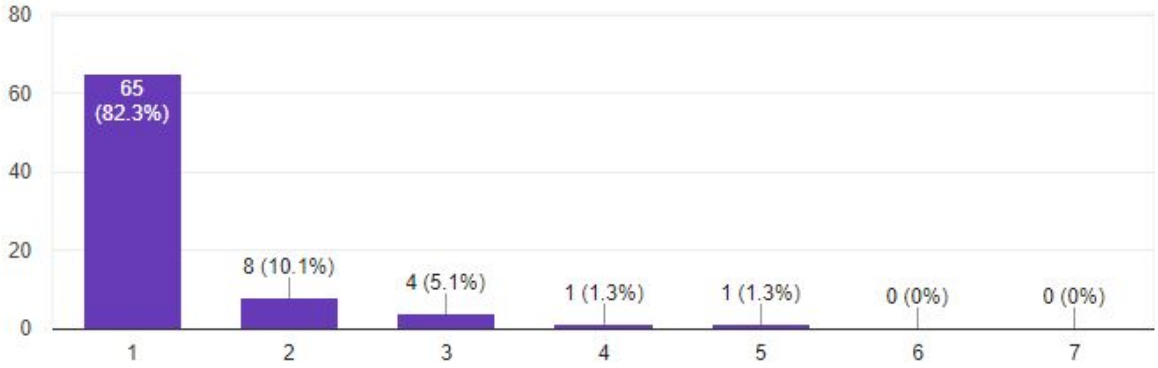
How do you feel about a company not taking any precautions to protect your financial data

79 responses



How do you feel about a company not taking any precautions to protect your personal data

79 responses



	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13

2	Gamer	0	3	1	1	1	1	1	1	1	1	1	1
3	Gamer	1	5	3	1	1	1	1	5	2	1	1	1
4	non-gamer							0	2	1	1	1	1
5	Gamer	0	3	2	2	1	1	0	3	1	1	1	1
6	Casual gamer	0	3	1	1	1	1	0	5	1	1	1	1
7	non-gamer							0	2	3	4	1	1
8	Gamer	1	5	5	6	3	2	1	5	6	5	5	5
9	Hardcore Gamer	0	6	1	1	1	1	0	6	1	1	1	1
10	Gamer	0	1	1	1	1	1	0	1	1	1	1	1
11	Gamer	0	2	2	1	1	1	0	1	2	1	1	1
12	Casual gamer	0	3	1	1	1	1	0	2	1	1	1	1
13	Hardcore Gamer	1	7	4	3	3	3	1	7	4	3	3	3
14	None of the other options							0	4	1	1	1	1
15	Hardcore Gamer	0	2	1	1	1	2	0	2	1	1	1	1
16	Gamer	0	2	1	1	1	1	0	1	2	1	1	1
17	non-gamer							0	4	1	1	1	1
18	Casual gamer	1	2	1	1	2	1	1	2	1	1	2	1
19	Hardcore Gamer	1	5	2	1	1	1	0	4	1	1	1	1

20	Gamer	1	4	2	1	1	1	0	4	3	1	1	1
21	Hardcore Gamer	1	4	3	2	2	2	1	5	4	2	2	2
22	Hardcore Gamer	1	5	2	1	1	2	1	5	4	1	1	1
23	Gamer	1	7	1	1	1	1	1	7	1	1	1	1
24	non-gamer							0	1	1	1	1	1
25	non-gamer							1	5	3	3	3	4
26	Hardcore Gamer	0	7	1	1	1	1	0	7	1	1	1	1
27	non-gamer							1	3	1	1	1	1
28	non-gamer							0	3	1	1	1	1
29	Casual gamer	1	6	4	4	5	3	0	6	3	3	2	2
30	Casual gamer	1	6	3	1	1	1	1	3	1	1	1	1
31	Casual gamer	1	5	1	1	1	1	0	3	1	1	1	1
32	Hardcore Gamer	1	7	5	1	1	1	1	7	2	1	1	1
33	Hardcore Gamer	1	6	1	2	1	1	0	2	1	1	1	1
34	Gamer	0	1	1	1	1	1	0	1	1	1	1	1
35	Casual gamer	0	4	1	1	1	1	0	4	1	1	1	1
36	Hardcore Gamer	1	4	1	1	1	1	1	4	1	1	1	1
37	non-gamer							0	1	1	1	1	1

38	None of the other options							0	1	1	1	1	1
39	Casual gamer	0	5	1	1	2	2	0	3	1	1	2	2
40	Gamer	1	7	1	1	1	1	1	4	1	1	1	1
41	Gamer	1	4	2	2	1	1	0	4	2	2	1	1
42	Casual gamer	1	6	3	3	1	1	1	7	1	1	1	1
43	Gamer	1	5	3	1	1	3	1	5	3	1	1	3
44	Hardcore Gamer	0	1	1	1	1	1	0	1	1	1	1	1
45	Gamer	1	5	2	2	1	1	1	5	2	1	1	1
46	Gamer	1	4	3	1	1	1	1	3	2	1	1	1
47	Gamer	0	2	1	1	1	1	0	1	1	1	1	1
48	Gamer	0	1	1	1	1	1	0	1	1	1	1	1
49	Hardcore Gamer	1	2	1	1	1	1	1	2	1	1	1	1
50	Hardcore Gamer	0	3	2	1	1	1	0	2	2	1	1	1
51	Casual gamer	0	7	1	1	1	1	0	1	1	1	1	1
52	Gamer	0	2	1	1	1	1	0	2	1	1	1	1
53	Hardcore Gamer	0	2	1	1	1	2	0	2	1	1	1	1
54	Hardcore Gamer	0	1	1	1	1	1	0	1	1	1	1	1
55	Gamer	0	1	1	1	1	1	0	1	1	1	1	1

56	Gamer	1	6	3	1	1	1	1	6	2	1	1	1
57	Gamer	0	2	1	1	1	1	0	1	1	1	1	1
58	Hardcore Gamer	0	2	1	1	1	1	0	1	1	1	1	1
59	Gamer	1	5	2	2	1	2	0	5	2	2	1	2
60	None of the other options							0	2	1	1	1	1
61	Hardcore Gamer	0	1	1	1	1	1	0	1	1	1	1	1
62	Hardcore Gamer	1	6	1	1	1	2	1	6	1	1	1	2
63	Casual gamer	1	6	5	4	4	3	1	6	4	4	4	3
64	Gamer	1	4	4	1	1	1	1	4	4	1	1	1
65	non-gamer							0	6	1	1	1	1
66	Gamer	1	5	3	2	1	2	1	6	3	1	1	2
67	Casual gamer	1	7	1	1	1	1	1	7	1	1	1	1
68	Gamer	0	1	1	1	1	1	0	2	2	2	2	2
69	Gamer	0	3	1	1	1	1	0	3	1	1	1	1
70	Casual gamer	0	1	1	1	1	1	0	2	1	1	1	1
71	Gamer	0	1	1	1	1	1	0	1	1	1	1	1
72	Gamer	0	6	2	1	1	3	1	6	2	1	1	3
73	Hardcore Gamer	1	6	4	2	1	4	1	5	4	1	1	1

74	Gamer	0	1	1	1	1	1	0	1	1	1	1	1
75	Casual gamer	1	7	7	1	1	1	1	7	7	1	1	1
76	Hardcore Gamer	0	1	1	1	1	1	0	1	1	1	1	1
77	Gamer	0	5	4	1	2	1	0	4	2	1	1	2
78	Gamer	0	4	2	2	1	1	0	4	1	1	1	1
79	Hardcore Gamer	1	6	3	1	1	1	1	6	2	1	1	1
80	Casual gamer	1	6	1	1	1	1	1	4	1	1	1	1

Q1 Which of the following categories do you match with the most

Q2 Would you give permission to a game company you have shared data with to share your data with other game companies?

Q3 How do you feel about the game company using the data you share with them

Q4 How do you feel about a game company releasing your personal data

Q5 How do you feel about a game company releasing your financial data

Q6 How do you feel about a game company not taking any precautions to protect your financial data

Q7 How do you feel about a game company not taking any precautions to protect your personal data

Q8 Would you give permission to a company you have shared data with to share your data with other companies?

Q9 How do you feel about a company using the data you share with them

Q10 How do you feel about a company releasing your personal data

Q11 How do you feel about a company releasing your financial data

Q12 How do you feel about a company not taking any precautions to protect your financial data

Q13 How do you feel about a company not taking any precautions to protect your personal data