



---

## Results

### Survey 55563

---

Number of records in this query:	277
Total records in survey:	277
Percentage of total:	100.00%





---

Field summary for swDevExp

Do you have any experience in software development?

---

Answer	Count	Percentage
Yes (A1)	184	66.43%
No (A2)	93	33.57%
No answer	0	0.00%

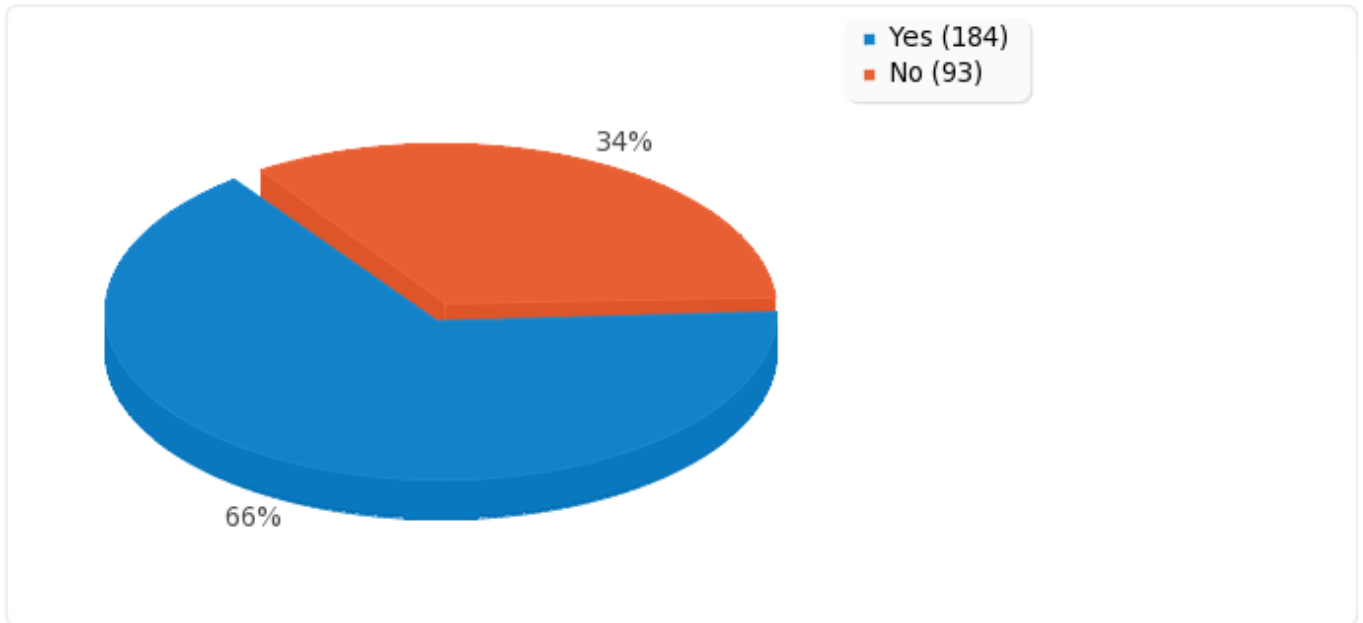


---

Field summary for swDevExp

Do you have any experience in software development?

---





---

Field summary for years

How long have you been doing software development?

---

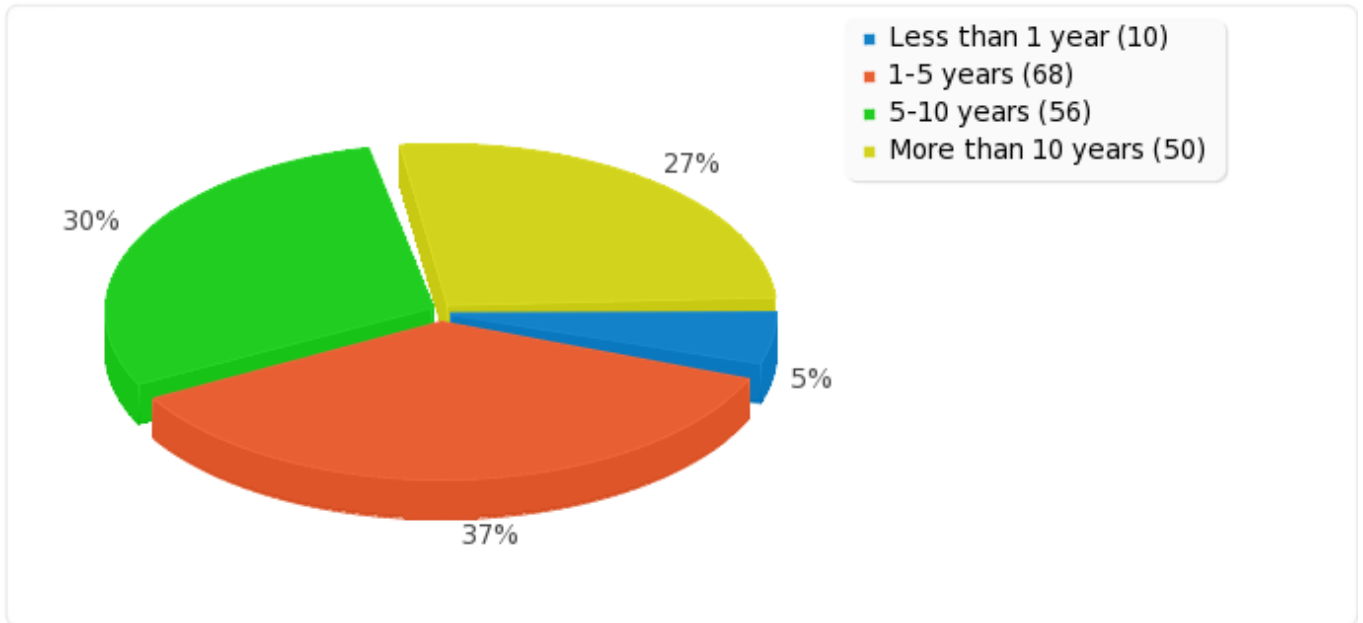
Answer	Count	Percentage
Less than 1 year (A1)	10	5.43%
1-5 years (A2)	68	36.96%
5-10 years (A3)	56	30.43%
More than 10 years (A4)	50	27.17%
No answer	0	0.00%



### Field summary for years

How long have you been doing software development?

---





---

Field summary for privacyImportant

How important is the privacy issue in such systems?

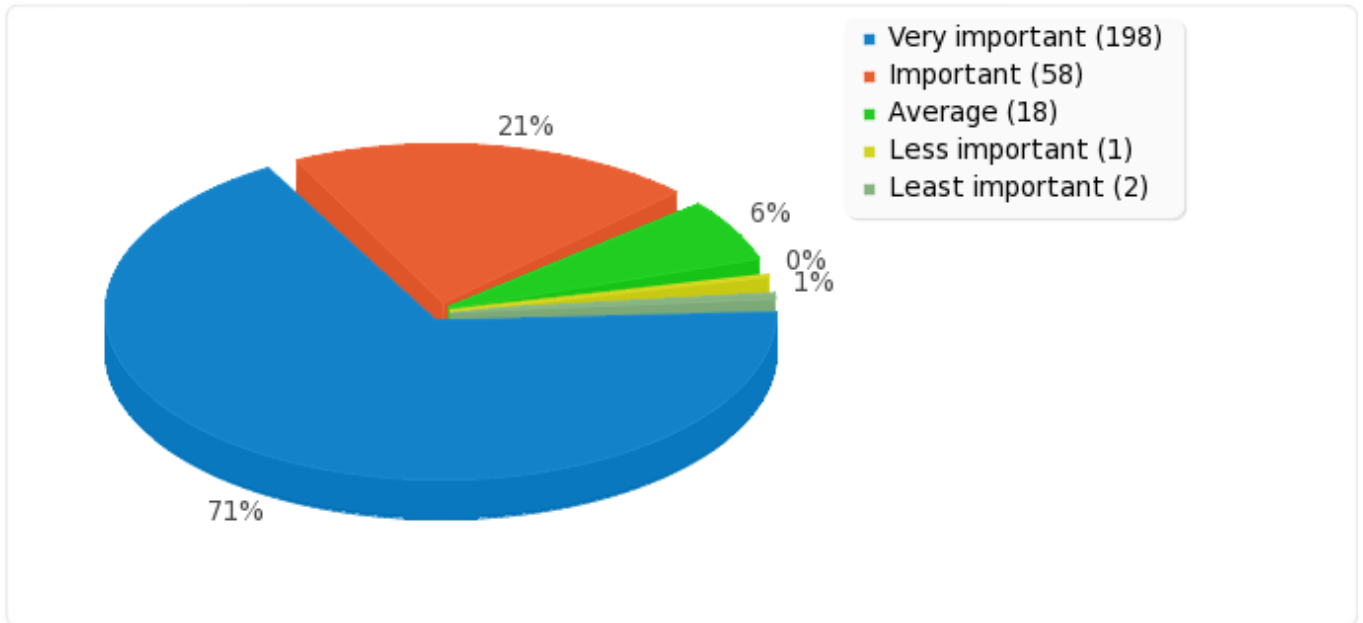
---

Answer	Count	Percentage
Very important (A2)	198	71.48%
Important (A3)	58	20.94%
Average (A4)	18	6.50%
Less important (A5)	1	0.36%
Least important (A6)	2	0.72%
No answer	0	0.00%



Field summary for privacyImportant

How important is the privacy issue in such systems?







---

Field summary for UuseIfPrivacyConcern

Would you be willing to use the system if you are worried about privacy issues?

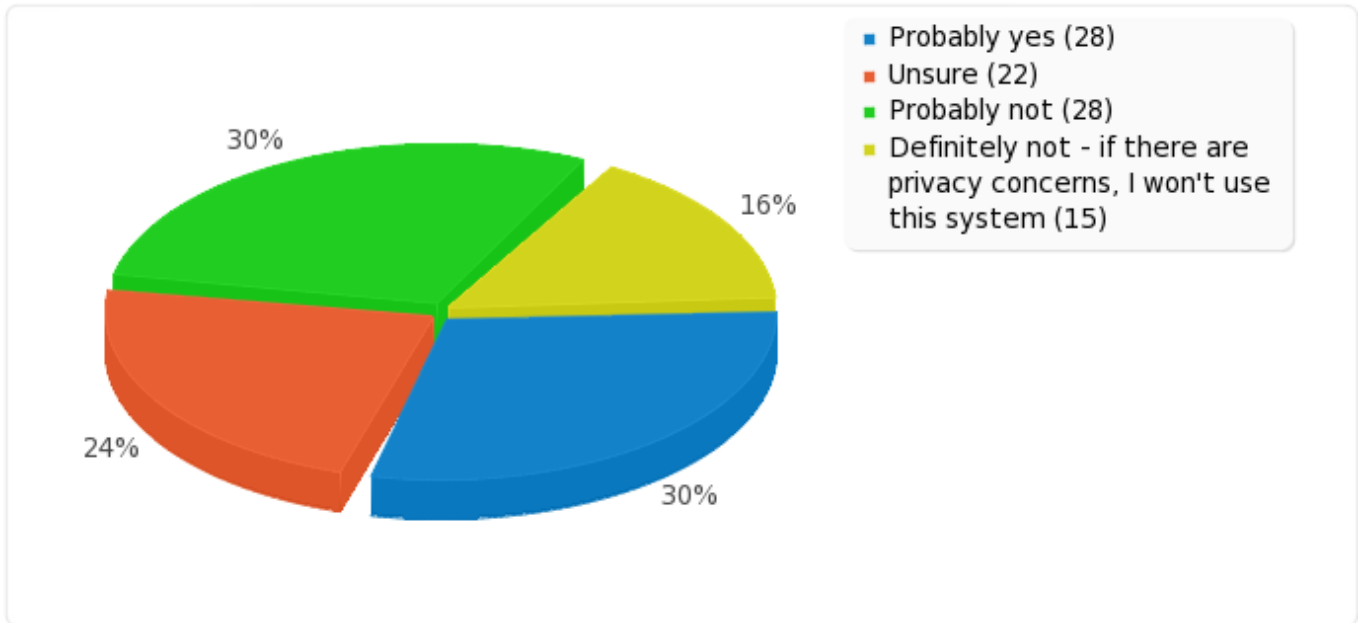
---

Answer	Count	Percentage
Definitely yes - I don't care about privacy (A1)	0	0.00%
Probably yes (A2)	28	30.11%
Unsure (A3)	22	23.66%
Probably not (A4)	28	30.11%
Definitely not - if there are privacy concerns, I won't use this system (A5)	15	16.13%
No answer	0	0.00%



Field summary for UuseIfPrivacyConcern

Would you be willing to use the system if you are worried about privacy issues?





---

Field summary for useIfPrivacyConcerns

Would users be willing to use your system if they are worried about privacy issues?

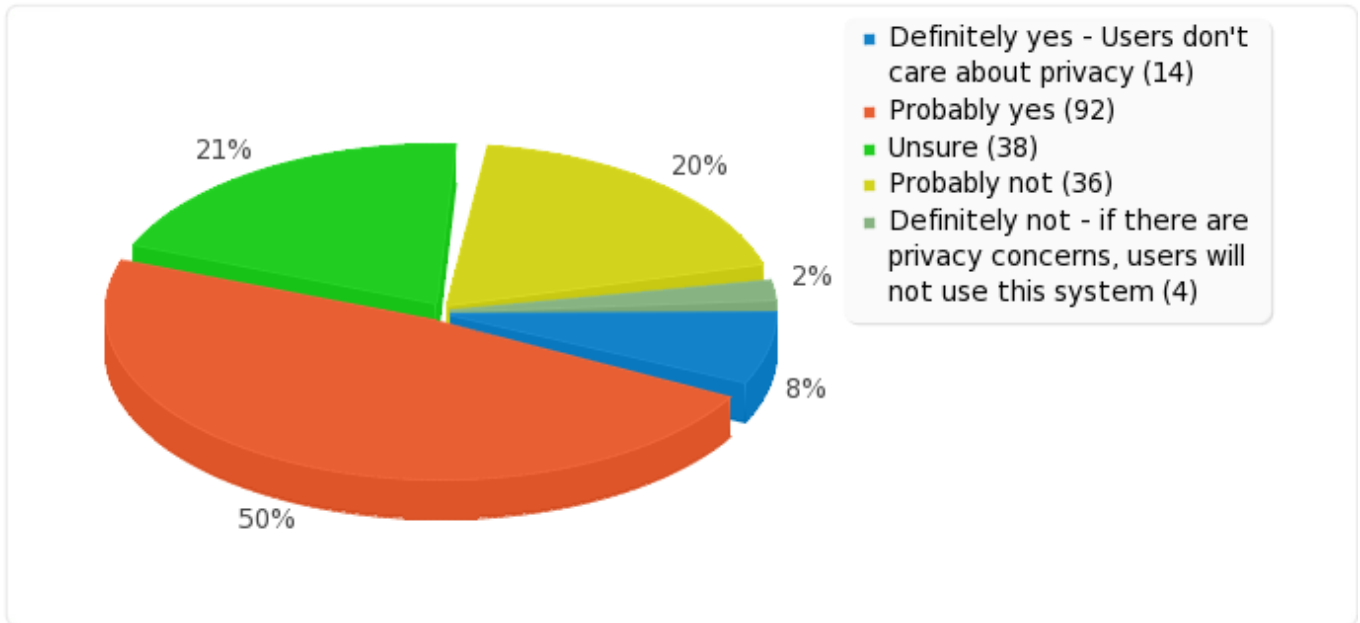
---

Answer	Count	Percentage
Definitely yes - Users don't care about privacy (A1)	14	7.61%
Probably yes (A2)	92	50.00%
Unsure (A3)	38	20.65%
Probably not (A4)	36	19.57%
Definitely not - if there are privacy concerns, users will not use this system (A5)	4	2.17%
No answer	0	0.00%



Field summary for useIfPrivacyConcerns

Would users be willing to use your system if they are worried about privacy issues?





---

Field summary for Uconcern(da)

Would the following increase privacy concerns?

[Data Aggregation: The system discovers additional information about you by aggregating data over a long period of time]

---

Answer	Count	Percentage
Yes (Y)	68	73.12%
No (N)	11	11.83%
Uncertain (U)	14	15.05%
No answer	0	0.00%

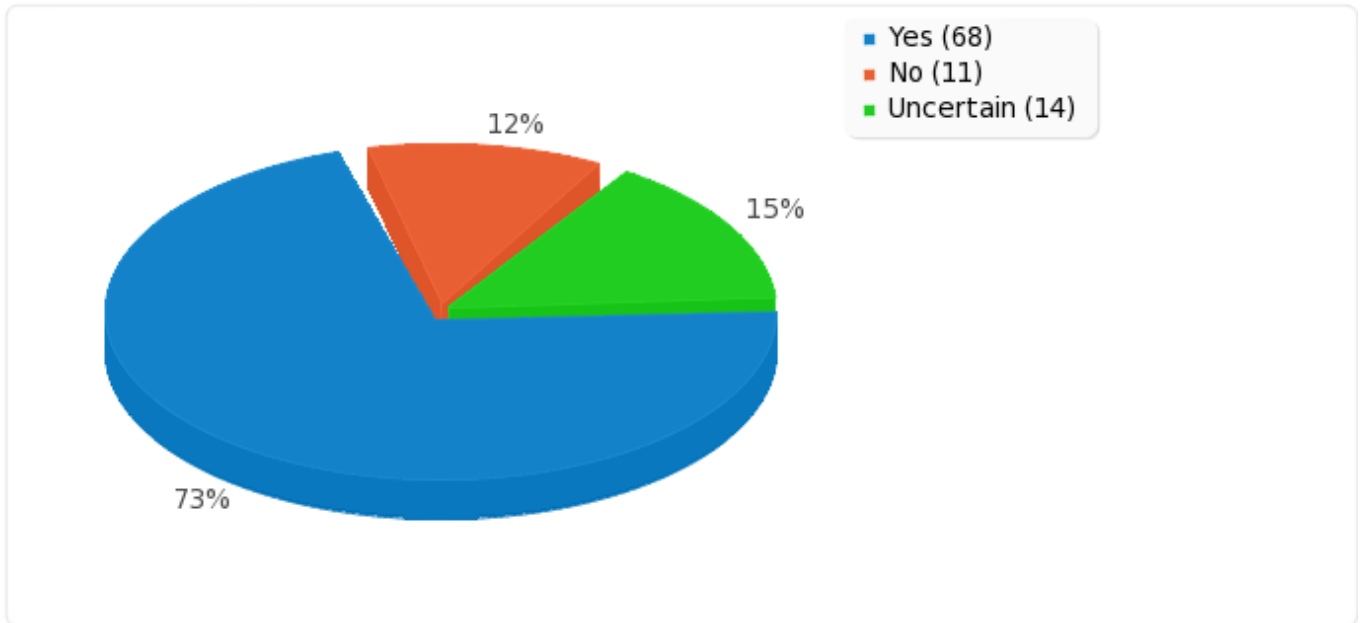


Field summary for Uconcern(da)

Would the following increase privacy concerns?

[Data Aggregation: The system discovers additional information about you by aggregating data over a long period of time]

---





---

Field summary for Uconcern(dd)

Would the following increase privacy concerns?

[Data Distortion: The system might misrepresent the data or your intent]

---

Answer	Count	Percentage
Yes (Y)	58	62.37%
No (N)	8	8.60%
Uncertain (U)	27	29.03%
No answer	0	0.00%

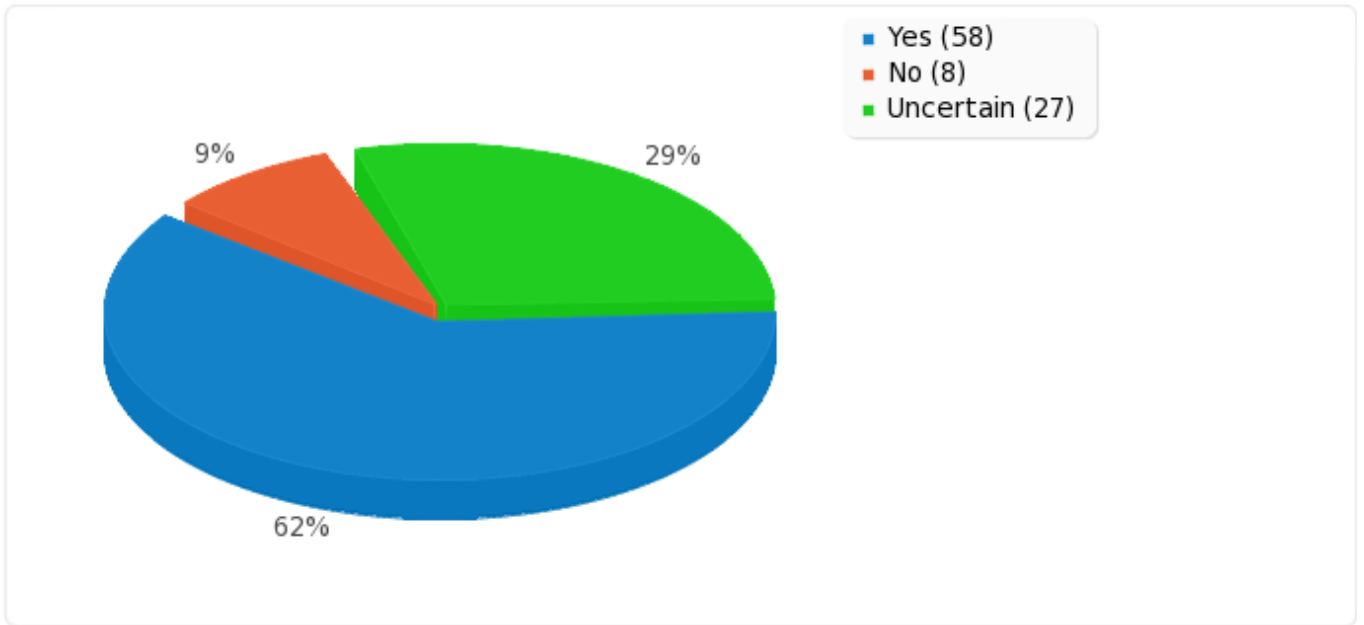


Field summary for Uconcern(dd)

Would the following increase privacy concerns?

[Data Distortion: The system might misrepresent the data or your intent]

---







---

Field summary for Uconcern(ds)

Would the following increase privacy concerns?

[Data Sharing: The collected data might be given to third parties for purposes like advertising]

---

Answer	Count	Percentage
Yes (Y)	76	81.72%
No (N)	5	5.38%
Uncertain (U)	12	12.90%
No answer	0	0.00%

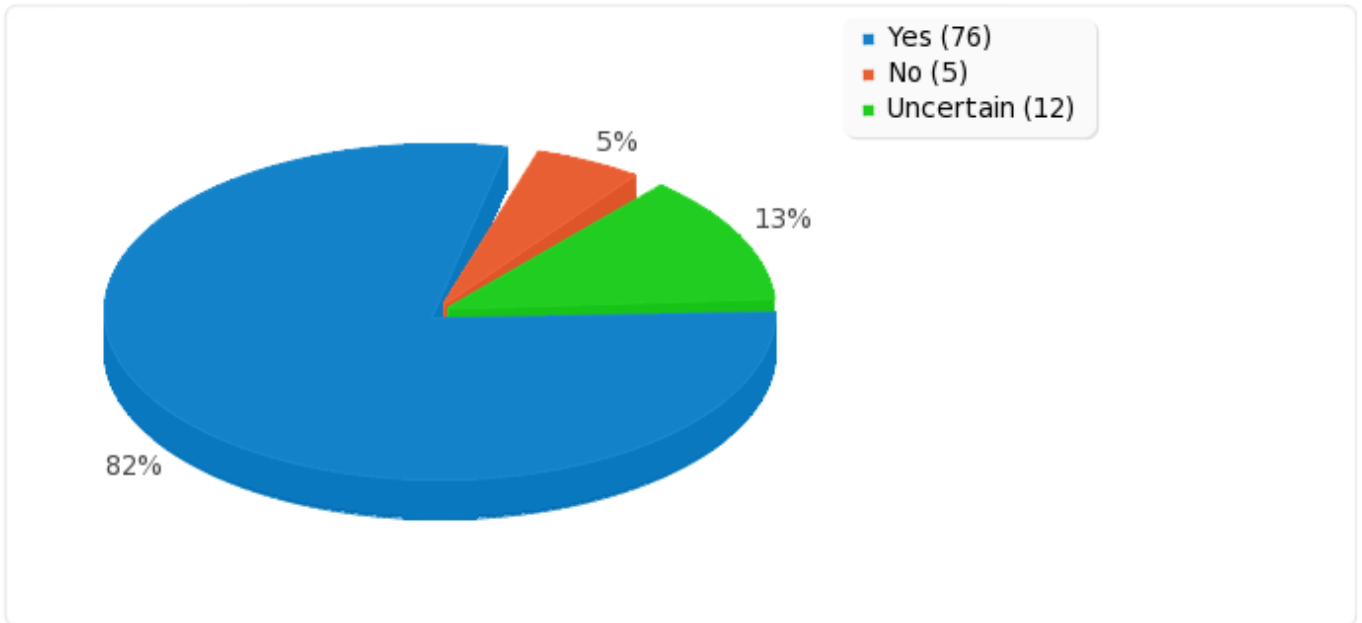


Field summary for Uconcern(ds)

Would the following increase privacy concerns?

[Data Sharing: [The collected data might be given to third parties for purposes like advertising]

---





---

Field summary for Uconcern(db)

Would the following increase privacy concerns?

[Data Breaches: Malicious users might get access to sensitive data about you (and other users)]

---

Answer	Count	Percentage
Yes (Y)	89	95.70%
No (N)	2	2.15%
Uncertain (U)	2	2.15%
No answer	0	0.00%

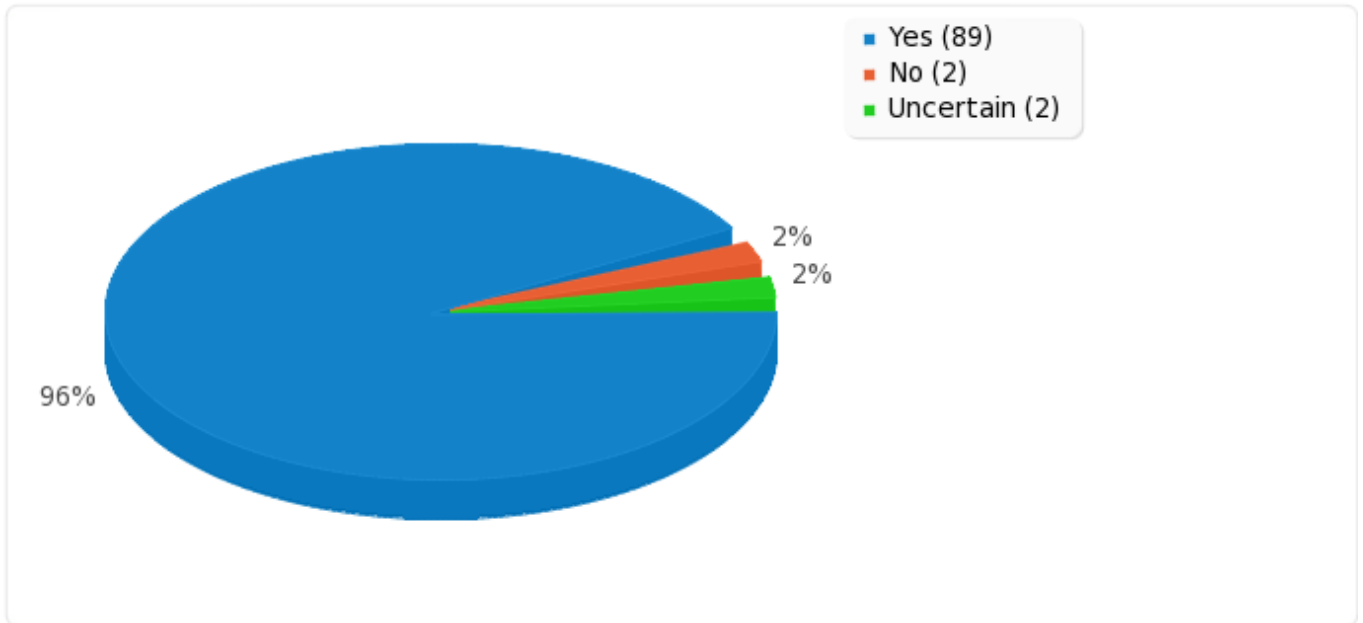


Field summary for Uconcern(db)

Would the following increase privacy concerns?

[Data Breaches: Malicious users might get access to sensitive data about you (and other users)]

---





---

Field summary for concern(da)

Would the following increase privacy concerns for users?

[Data Aggregation: The system discovers additional information about the user by aggregating data over a long period of time]

---

Answer	Count	Percentage
Yes (Y)	88	47.83%
No (N)	48	26.09%
Uncertain (U)	48	26.09%
No answer	0	0.00%

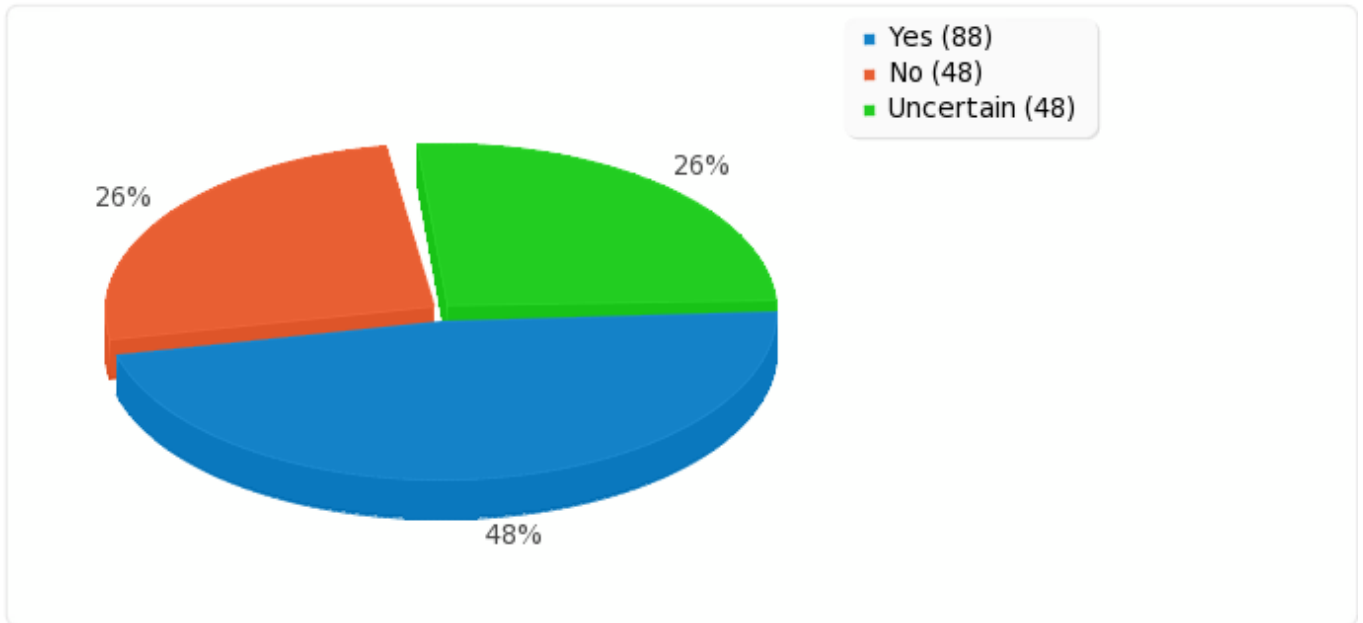


Field summary for concern(da)

Would the following increase privacy concerns for users?

[Data Aggregation: The system discovers additional information about the user by aggregating data over a long period of time]

---





---

Field summary for concern(dd)

Would the following increase privacy concerns for users?

[Data Distortion: The system might misrepresent the data or user intent]

---

Answer	Count	Percentage
Yes (Y)	87	47.28%
No (N)	38	20.65%
Uncertain (U)	59	32.07%
No answer	0	0.00%

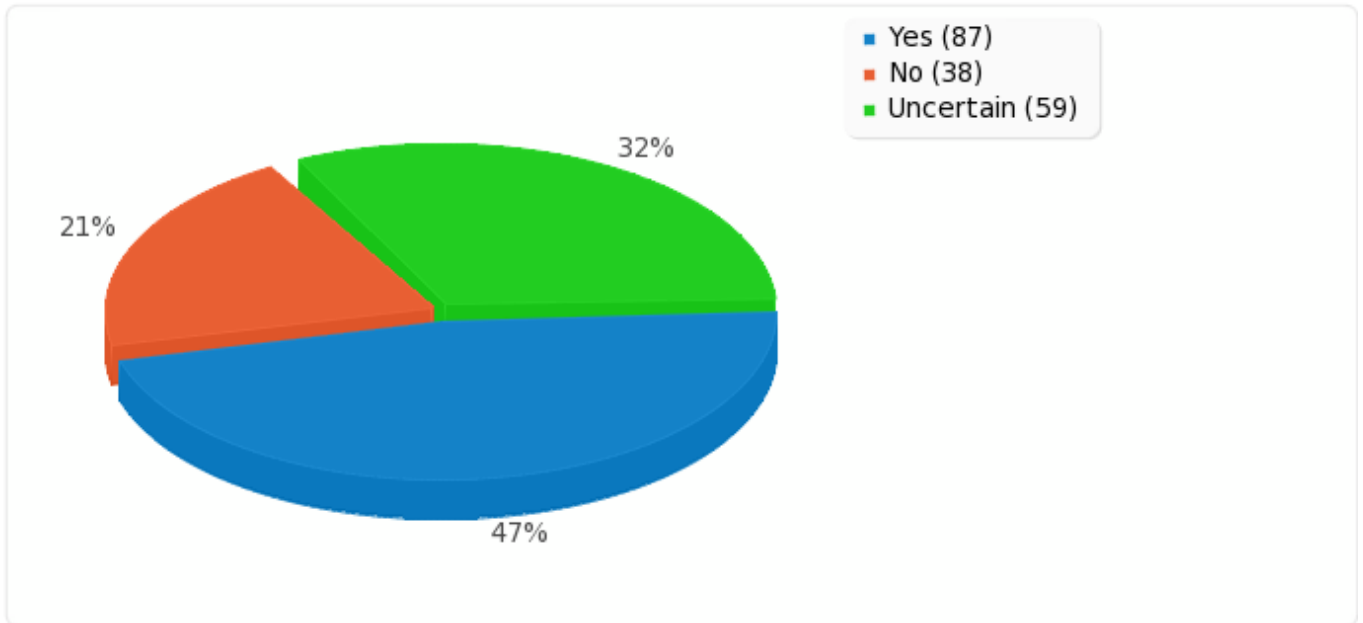


Field summary for concern(dd)

Would the following increase privacy concerns for users?

[Data Distortion: The system might misrepresent the data or user intent]

---







---

Field summary for concern(ds)

Would the following increase privacy concerns for users?  
[Data Sharing: The collected data might be given to third parties for purposes like advertising]

---

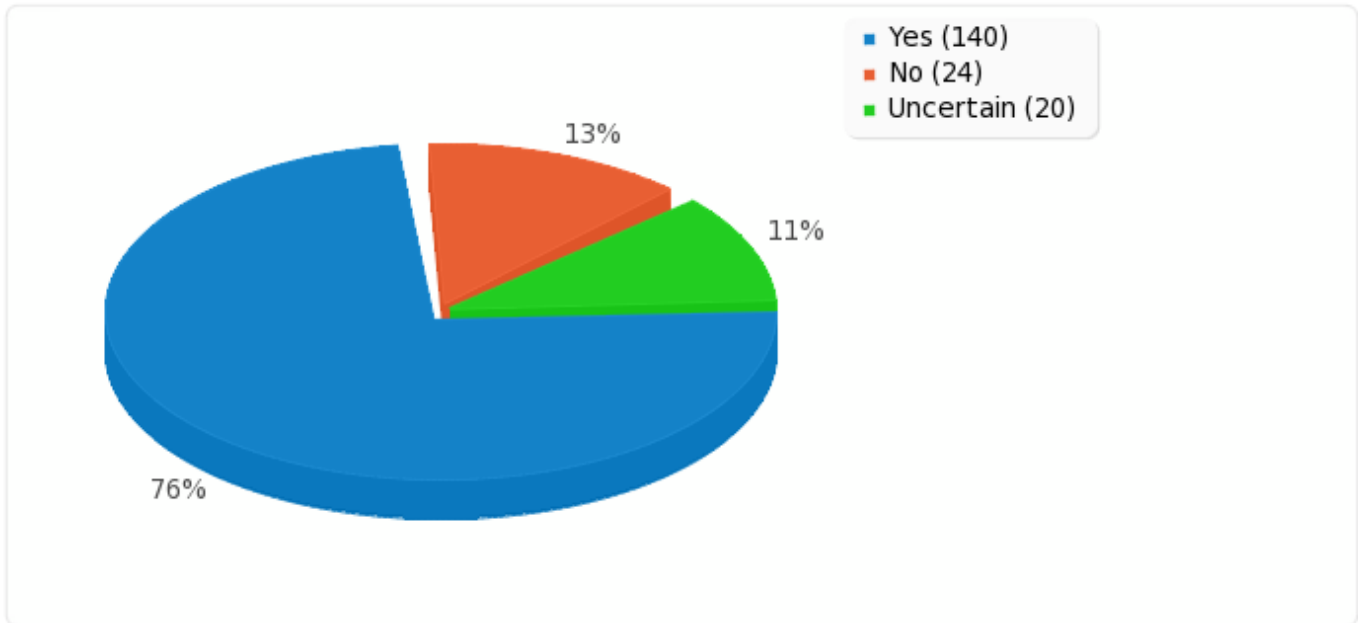
Answer	Count	Percentage
Yes (Y)	140	76.09%
No (N)	24	13.04%
Uncertain (U)	20	10.87%
No answer	0	0.00%



Field summary for concern(ds)

Would the following increase privacy concerns for users?  
[Data Sharing: The collected data might be given to third parties for purposes like advertising]

---





---

Field summary for concern(db)

Would the following increase privacy concerns for users?

[Data Breaches: Malicious users might get access to sensitive data about other users]

---

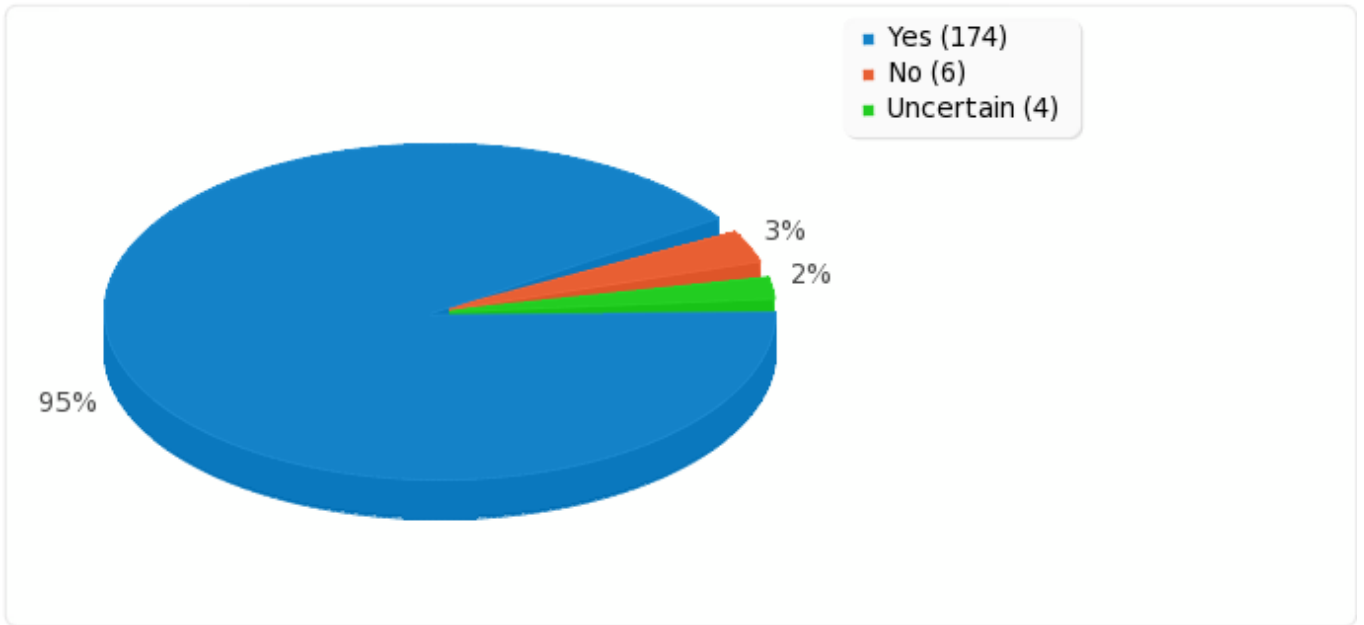
Answer	Count	Percentage
Yes (Y)	174	94.57%
No (N)	6	3.26%
Uncertain (U)	4	2.17%
No answer	0	0.00%



Field summary for concern(db)

Would the following increase privacy concerns for users?

[Data Breaches: Malicious users might get access to sensitive data about other users]





## Field summary for additionalConcerns

Do you have additional privacy concerns? Why?

Answer	Count	Percentage
Answer	53	19.13%
No answer	224	80.87%

## Responses

- Langzeitspeicherung (keine Möglichkeit, eigene Daten wieder zu löschen)

Data Acquisition - Company A has a decent privacy policy, Company B acquires the company, and in doing so, now has access to Company A's data.

Die Daten können von Hackern (staatlich und/oder kriminell) ausgespäht und dann missbraucht werden. Behörden könnten soziale Daten für Social Profiling nutzen.

Verknüpfung von Daten aus unterschiedlichen Quellen, ohne dass der Nutzer weiß, dass dies geschieht bzw. dass dies unterschiedlichen Quellen miteinander in Beziehung gesetzt werden.

Veröffentlichung von persönlichen Daten (nicht nur die Weitergabe zu Werbezwecken).

I am not just concerned with a web company giving my data to third parties, but also receiving data from third parties, such as Facebook getting data from pharmacy loyalty cards.

Nein.

nein leider fallen mir keine weiteren ein.

NO

No

I think the desirability of the system is an important influence on users' willingness to use it amidst privacy concerns. Cf. social pressure / critical mass effect in Facebook.

Many. Not personally me, but my numerous paranoid friends, for obvious reasons.

I would have additional privacy concerns about the correctness of the privacy system's implementation.

Die Verfügbarkeit steht für den Laien im Alltag an erster Stelle. Sicherheit wird zwar diskutiert aber am Ende nicht angewandt.

oft Erfassung für den Prozess/Betreiber unnötiger/überflüssiger Daten (Widerspruch zur Datensparsamkeit/-erfordernis im deutschen/EU DS-Gesetz) --> Profilbildung

Abruf der Daten durch in- und ausländische staatliche Behörden, Geheimdienste

Mitarbeiter haben Zugriff auf Daten. Sind die Daten wieder vollständig löschar?

gradual degradation of equality:

(erroneously) collected and (erroneously) aggregated information that is used to (erroneously) profile people and (accidentally) discriminate against certain classes by systematically depriving them of certain choices.

Everybody is guilty of something or has made grave mistakes - your enemies should not have an easy time digging all that information



up, otherwise everybody can be shot down with words within the blink of an eye.

Versehentliche Veröffentlichung von Daten -> Nicht immer stecken "böswillige Nutzer" dahinter, sondern sogenannte "Freunde". Darin sehe ich das größte Risiko, da viele sich einfach nichts dabei denken...

Datenverlust (würde man eher unter Datensicherheit und nicht unter Datenschutz thematisieren, aber im Deutschen ist das für mich nicht so klar getrennt wie im Englischen Security vs. Privacy) -> Das hat durchaus auch mit Sicherheit zu tun, ob mir ein Online-Tool irgendwelche Export-Funktionen bietet, damit ich meine Daten auch behalte, wenn das Tool in fünf bis zehn Jahren abgeschaltet wird, oder ob ich meine Daten "abtrete" (dann wird irgendwer sie aufkaufen, wenn die Firma insolvent ist, und ich habe keinen Einfluss darauf.)

Daten aus unterschiedlichen Systemen werden verknüpft. Hierdurch gewinnen sie bedeutend an Aussagekraft. Da schwer nachzuvollziehen ist, welche Dienste untereinander Daten austauschen, ist das Ausmaß dieses Problems schwer abzuschätzen und noch schwerer zu vermitteln.

Concern of retargeting. At random times, I am confronted online with products/content I viewed before without having control of when it is displayed. When sharing a PC-laptop-ipad I don't want that information to be displayed to other users.

Durch Aggregation von Daten aus diesem und weiteren Systemen könnten umfassendere Informationen über die Benutzer gewonnen werden.

anyway there is prism :~)

Behördliche oder staatlicher Datenzugriff, unkontrollierte Datentransparenz; Zugriff und Verwendung durch Geheimdienste, Presse oder Journalisten.

Personal identification for systems not explicitly tied to identity (e.g., pseudonymous forums, search engines).

Having the data made public if it was not intended to be (e.g., Amazon purchase history, Facebook private messages).

Privacy in take an advantage of user data without permission like advertisement, HIPPA and many other issues found in Google, Facebook and today web applications.

the system might make use of my data to infer data about my community, my network of contact, not only about me (as a user).

I liked your point on the misinterpretation of data, i.e. the gathering of data per se might have no privacy concern, but the seeing how it was interpreted might do. Example, Youtube which sometimes gives you suggestion has nothing to do with your intention using its wonderful collaborative filtering mechanisms.

Das größte Problem ist meiner Meinung nach die (vielleicht auch nur gefühlte) Intransparenz eines solchen Systems. Der Nutzer weiss schlicht und einfach nicht welche Daten gespeichert und wie sie dann genutzt werden. Dazu kommt ein grundlegendes Technikunverständnis in der breiten Öffentlichkeit, was dazu führt, das auch irrationale Ängste oder Befürchtungen entstehen.

No; data breaches and sharing are my biggest concerns.

lack of legislation concerning personal data protection in the country of developer/host of data base  
Anything that they collect that is not completely anonymized is a



concern for me. I don't like them collecting data on my that I didn't explicitly authorize.

Government access is not exactly a data breach, but still a privacy concern.

Es ist einfach. Hätte Hitler diese Daten gehabt, hätten nich 10, sonder 60 Millionen Menschen wegen seines widerwärtigen Systems das Leben verloren.

Ich wünsche es mir sicher nicht, halte es aber für naiv zu glauben, dass es nicht auch andere bösartige Menschen gibt, die dies dann durchziehen würden. Da man dies leider nicht ausschließen kann, ist es grundsätzlich gefährlich, diese Daten überhaupt zu speichern.

Nutzung von Datenaggregation, um ökonomische Vorteile zu erzielen, Überteuerung von Produkten für die man sich interessiert etc.

Yes. Data sharing for non-advertising purposes - government programs, employers (or other entities) for various types of information obtained directly (location, preferences etc.) or through aggregation (behavior/personality analysis in relation to social network)

Why? Because a part of the sharing of information is not straight-forward or difficult to control. E.g. Not straight-forward: sometimes sharing sensitive data is activated by default in applications (unaware users would leave it so).

Difficult : face recognition in photos (how can one be sure no algorithm is running in the background collecting data?), inferred information from social networks (who are the friends, what are there preferences etc.)

It is not enough clear who sees the users data.

Yes.

Because online data is used to monitor the opinions and behavior of citizens.

Because there are companies/governments creating fake identities online to try to manipulate public opinion.

Because whenever something happen the media uses their data accessible online to 'sell' this person as good or evil.

Data storage: Collecting the data and storing for a long period of time is seen more critical than just collecting. Additionally, depending in the data, the storage location might make a huge difference.

Anonymous data: Is the data collected and stored or analyzed in an anonymous way? If so, people would be more likely to disregard their concern. Independent from the actual behavior.

Transparency: transparency and letting the user choose make a huge difference. Maybe not in the beginning and maybe not for all users but definitely for a specific user group.

Data collected without my awareness

Einmal preisgegebene Daten können nicht mehr zurückgenommen oder von mir selbst gelöscht werden. Selbst wenn mir die Löschung meiner Daten zugesagt würde, könnte ich dies nicht kontrollieren.

Datenaggregation über Dienste hinweg - gerade die Verknüpfung von Daten, die bei verschiedenen Dienstleistungen anfallen, die nichts miteinander zu tun haben, ermöglicht die Erstellung von intimen, vollständigen Persönlichkeitsprofilen: mein Buchhändler muss nicht wissen, was für Suchanfragen ich im Internet verwende, mein E-Mail-Anbieter braucht keinen Zugriff auf meinen Bezahltdienst, ein Musikanbieter wie iTunes braucht sich nicht für mein Adressbuch zu interessieren.

no



All of these issues concern me, but they don't necessarily make me quit using the programs. There is a measure of risk in most social media programs I'm sure.

Yes. I don't want data compiled on me. I don't want someone else to get it and be able to use it against me. RFID cards, RFID in license plates and driver's licenses. Phone security, etc.

persistence of data over time might lead to conflicts with future audiences that I cannot assess at the moment of data disclosure - continuous monitoring, combined with aggregation over multiple channels or sources, leads to complex user profiling and it's disturbing to know that your life is monitored on so many levels, and so many people might know more about you that you can ever dream

information sharing, user profiling, unofficial third parties (intelligence community)

Die Verbindungen zwischen Menschen/Accounts und deren Interessen kann zu einem Problem führen, da dann gezielt Menschengruppen angesprochen oder manipuliert werden können. Das geht zwar in Richtung personalisierte Werbung, ist allerdings noch einmal schlimmer.

Weitergabe der Daten an Dienstleister mit geringerem Schutz & unter anderer Gesetzgebung. Beispiele: Retargeting-Anbieter, Web-Analytics-Anbieter usw

Eingebundene Skripte von externen Seiten unterliegen nicht dem gleichen Schutz & Überwachung & Sorgfalt wie eigene Server

Dass Daten nicht endgültig und dauerhaft gelöscht werden können.

Speicherung von daten in unkontrollierten Clouds wo Mandantentrennung bedingt möglich ist. Umbedingte Weitergabe der Daten für Verfassungsschutz und Terrorismusbekämpfung.

I have concerns regarding secret services like the NSA

Weitergabe der Daten an Geheimdienste wie die NSA.

Bei der Weitergabe zwecks Werbezwecken finde ich kommt es auf die Transparenz für den Nutzer und die Art der Daten an! Weiß der Nutzer ganz klar, welche Daten weitergegeben werde, hätte ich keine grundsätzlichen Datenschutzbedenken. Der Benutzer muss dann natürlich noch entscheiden, stimmt er der Weitergabe zu oder verzichtet er auf den Dienst!

Authorities looking into my data

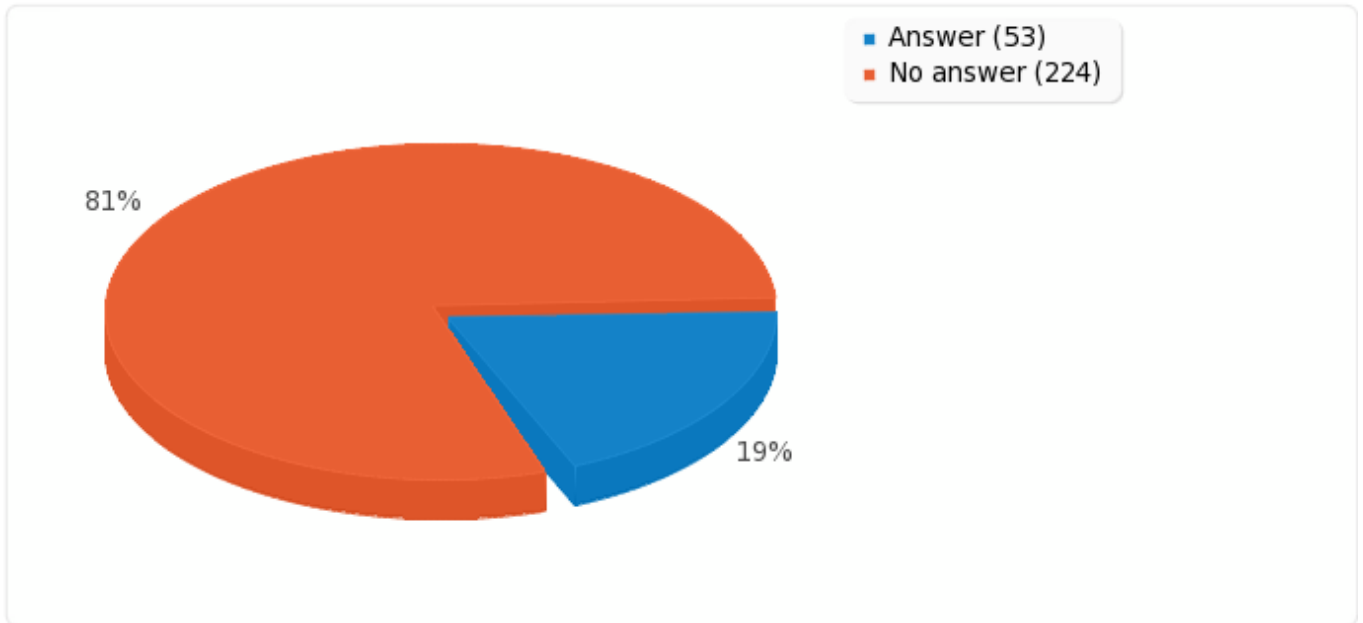




Field summary for additionalConcerns

Do you have additional privacy concerns? Why?

---





---

### Field summary for concernLocation

Do your concerns about privacy depend on the location where the data is stored - e.g., on your computer as opposed to a server in a different country?

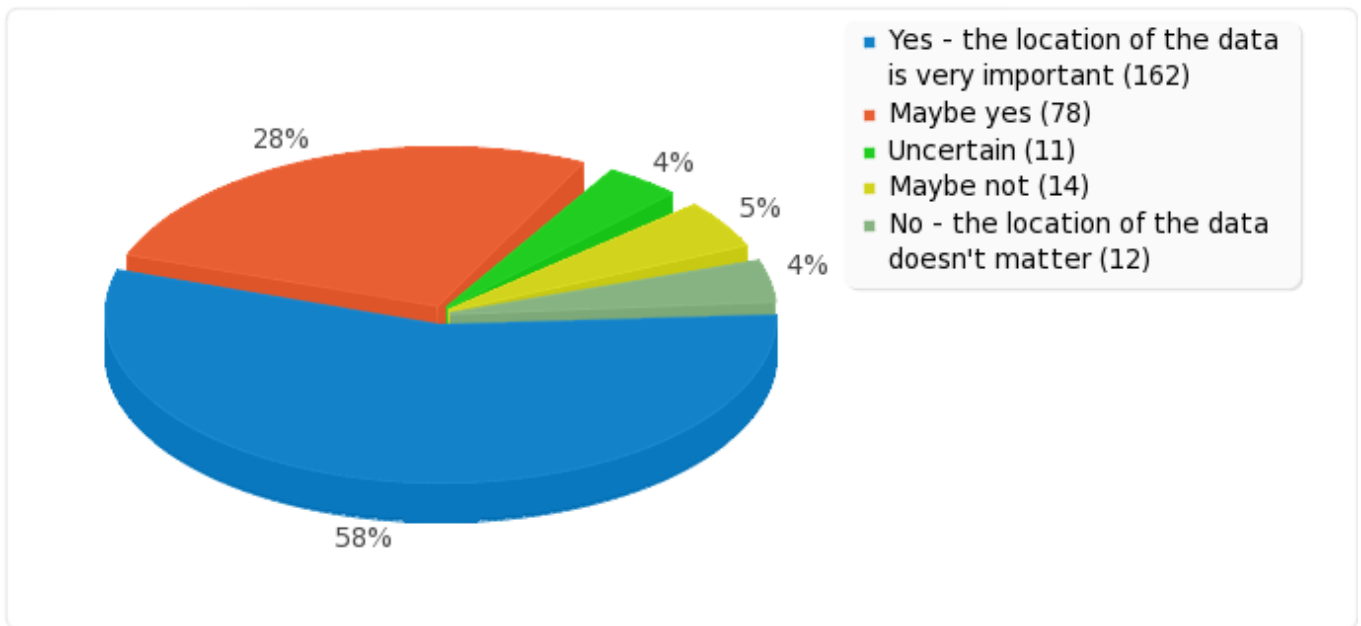
---

Answer	Count	Percentage
Yes - the location of the data is very important (A1)	162	58.48%
Maybe yes (A2)	78	28.16%
Uncertain (A3)	11	3.97%
Maybe not (A4)	14	5.05%
No - the location of the data doesn't matter (A5)	12	4.33%
No answer	0	0.00%



Field summary for concernLocation

Do your concerns about privacy depend on the location where the data is stored - e.g., on your computer as opposed to a server in a different country?





---

Field summary for UreduceConcern(polic)

Would the following measures help in reducing concerns about privacy?  
[Privacy Policy, License Agreements, etc. [Describing what the system  
will/won't do with the data]

---

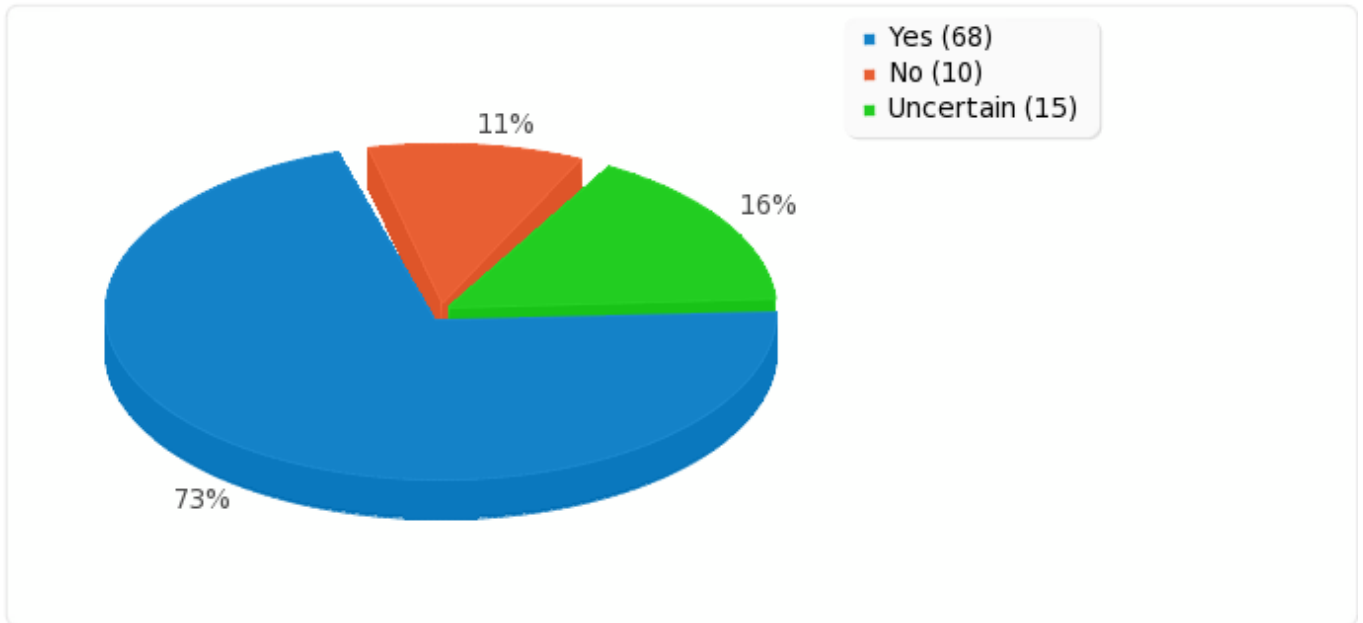
Answer	Count	Percentage
Yes (Y)	68	73.12%
No (N)	10	10.75%
Uncertain (U)	15	16.13%
No answer	0	0.00%



Field summary for UreduceConcern(polic)

Would the following measures help in reducing concerns about privacy?  
[Privacy Policy, License Agreements, etc. [Describing what the system  
will/won't do with the data]

---





---

Field summary for UreduceConcern(law)

Would the following measures help in reducing concerns about privacy?  
[Privacy Laws []Describing which national law the system is complaint with  
(e.g., HIPAA in the US, European privacy laws)]

---

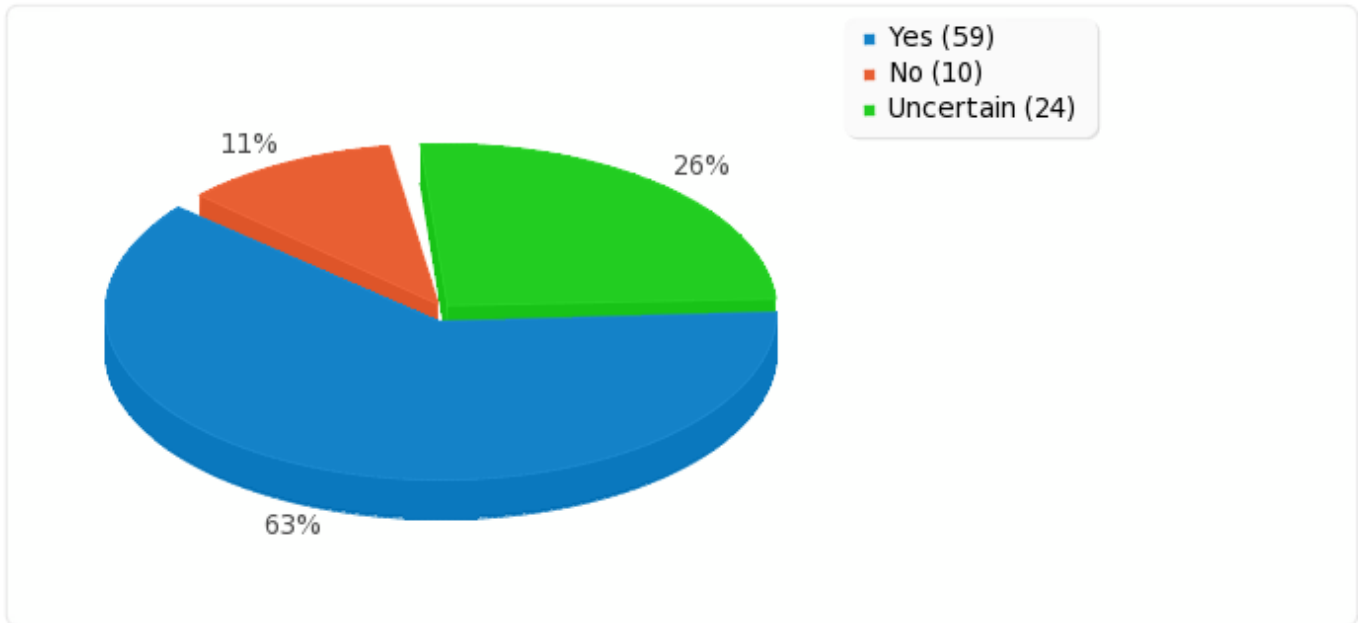
Answer	Count	Percentage
Yes (Y)	59	63.44%
No (N)	10	10.75%
Uncertain (U)	24	25.81%
No answer	0	0.00%



Field summary for UreduceConcern(law)

Would the following measures help in reducing concerns about privacy?  
[Privacy Laws [Describing which national law the system is complaint with  
(e.g., HIPAA in the US, European privacy laws)]

---





---

Field summary for UreduceConcern(anon)

Would the following measures help in reducing concerns about privacy?  
[Anonymizing all data □ Ensuring that none of the data has any personal identifiers]

---

Answer	Count	Percentage
Yes (Y)	77	82.80%
No (N)	9	9.68%
Uncertain (U)	7	7.53%
No answer	0	0.00%

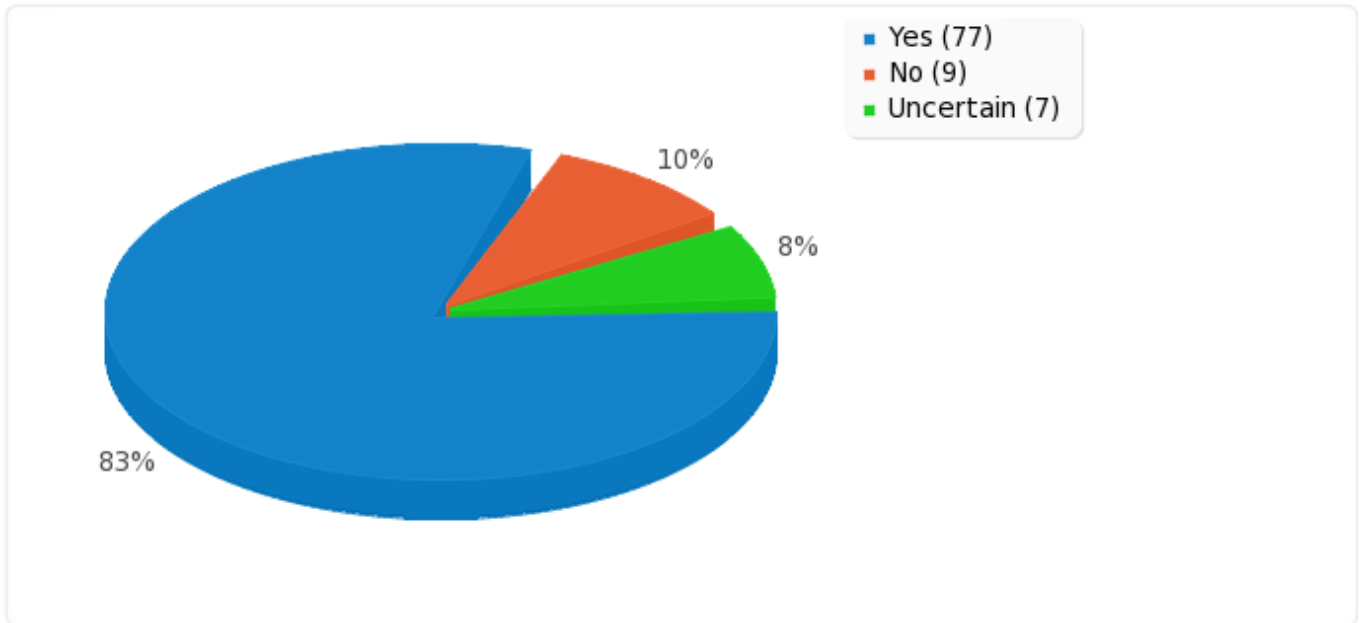




Field summary for UreduceConcern(anon)

Would the following measures help in reducing concerns about privacy?  
[Anonymizing all data [ Ensuring that none of the data has any personal  
identifiers]

---





---

Field summary for UreduceConcern(check)

Would the following measures help in reducing concerns about privacy?  
[Please select "Yes " for this row]

---

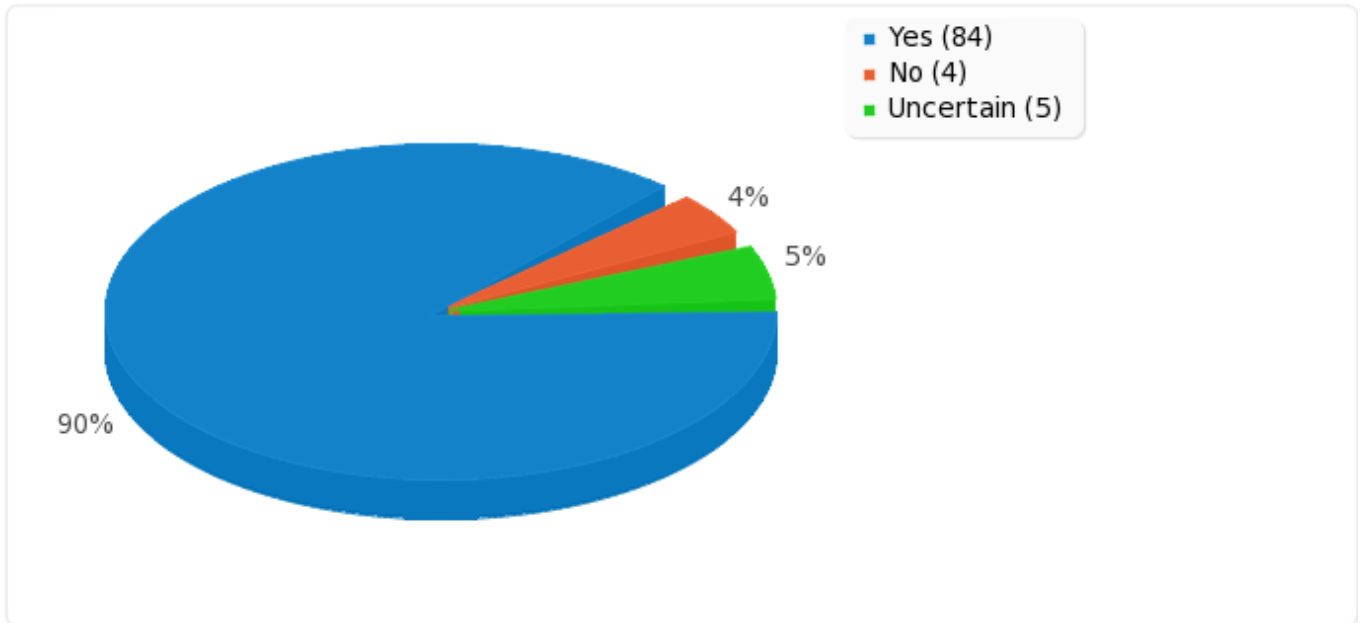
Answer	Count	Percentage
Yes (Y)	84	90.32%
No (N)	4	4.30%
Uncertain (U)	5	5.38%
No answer	0	0.00%



Field summary for UreduceConcern(check)

Would the following measures help in reducing concerns about privacy?  
[Please select "Yes " for this row]

---





---

Field summary for UreduceConcern(tech)

Would the following measures help in reducing concerns about privacy?  
[Technical Details [Describing the algorithms/source code of the system in order to achieve higher trust (E.g., encryption of data)]]

---

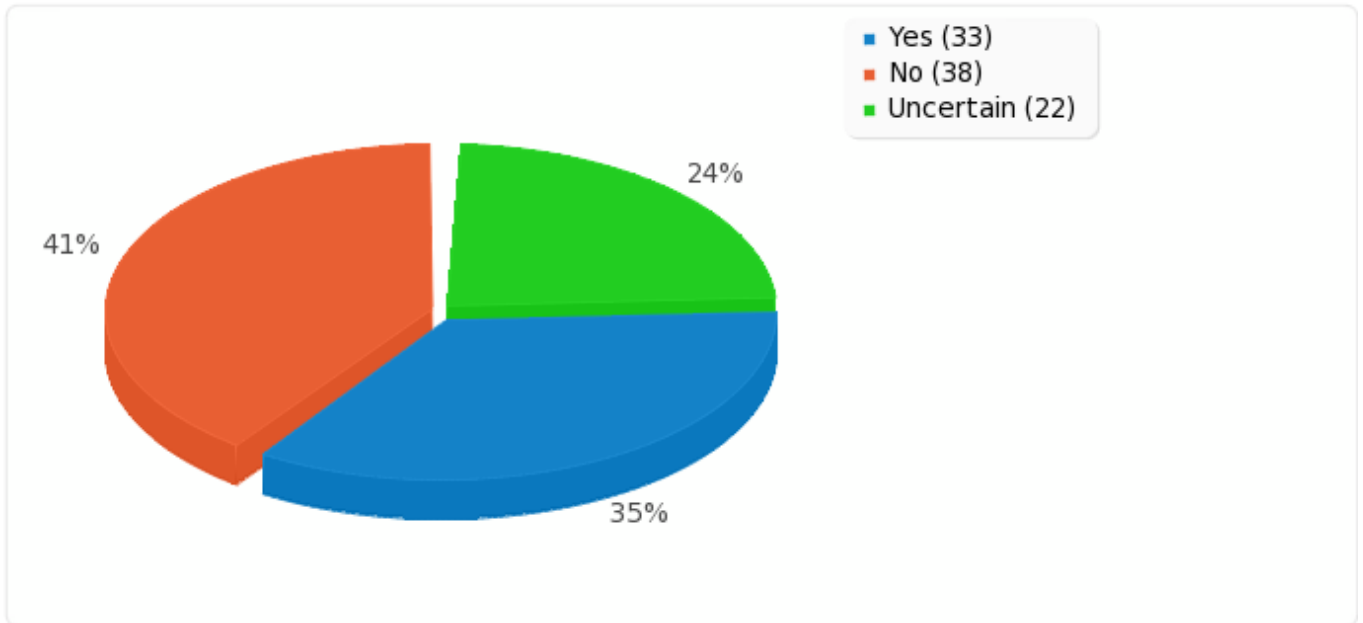
Answer	Count	Percentage
Yes (Y)	33	35.48%
No (N)	38	40.86%
Uncertain (U)	22	23.66%
No answer	0	0.00%



Field summary for UreduceConcern(tech)

Would the following measures help in reducing concerns about privacy?  
[Technical Details [Describing the algorithms/source code of the system in order to achieve higher trust (E.g., encryption of data)]]

---





---

Field summary for UreduceConcern(usage)

Would the following measures help in reducing concerns about privacy?  
[Details on usage ¶ Describe, e.g., in a table how different data are used]

---

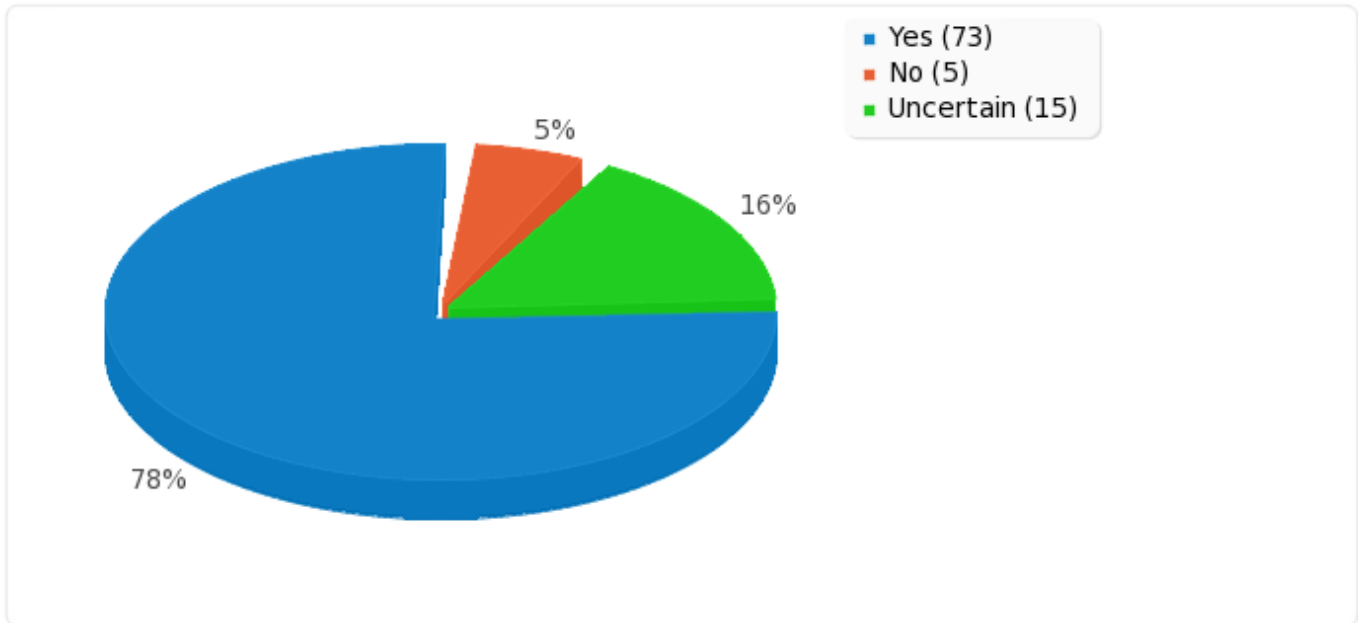
Answer	Count	Percentage
Yes (Y)	73	78.49%
No (N)	5	5.38%
Uncertain (U)	15	16.13%
No answer	0	0.00%



Field summary for UreduceConcern(usage)

Would the following measures help in reducing concerns about privacy?  
[Details on usage ¶Describe, e.g., in a table how different data are used]

---





---

Field summary for reduceConcern(polic)

Would the following measures help in reducing user concerns about privacy?  
[Privacy Policy, License Agreements, etc. [Describing what the system  
will/won't do with the data]

---

Answer	Count	Percentage
Yes (Y)	103	55.98%
No (N)	36	19.57%
Uncertain (U)	45	24.46%
No answer	0	0.00%

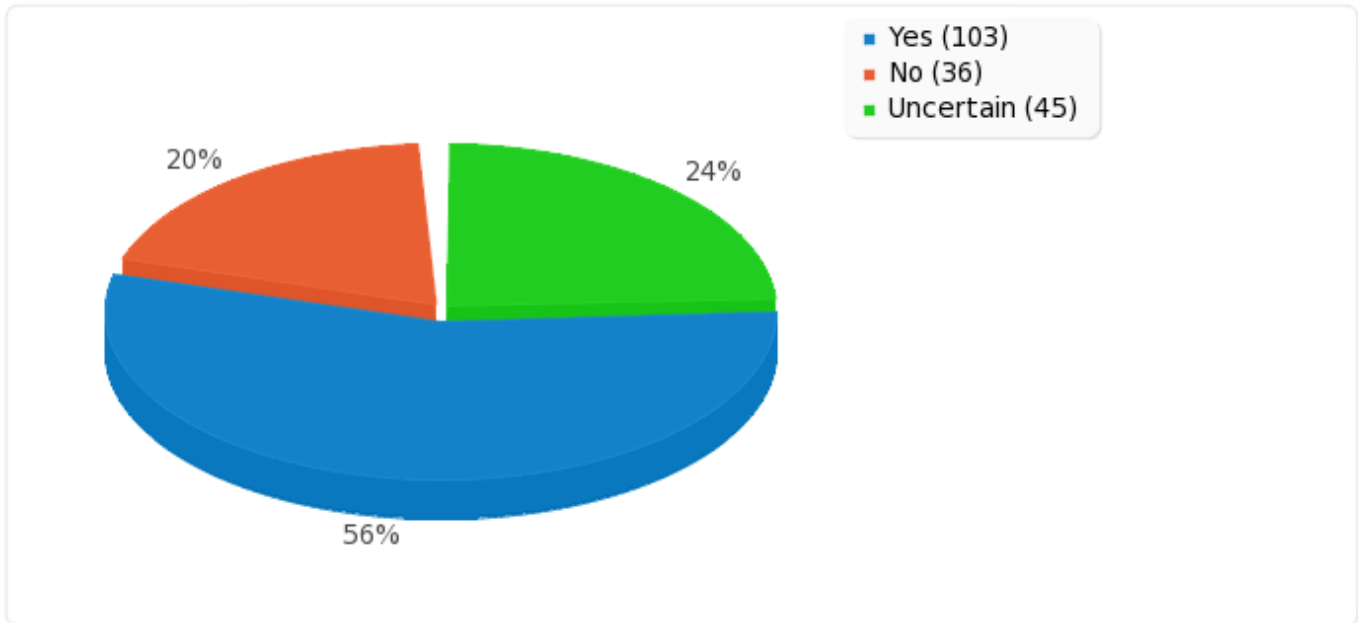




Field summary for reduceConcern(polic)

Would the following measures help in reducing user concerns about privacy?  
[Privacy Policy, License Agreements, etc. [Describing what the system  
will/won't do with the data]

---





---

Field summary for reduceConcern(law)

Would the following measures help in reducing user concerns about privacy?  
[Privacy Laws []Describing which national law the system is complaint with  
(e.g., HIPAA in the US, European privacy laws)]

---

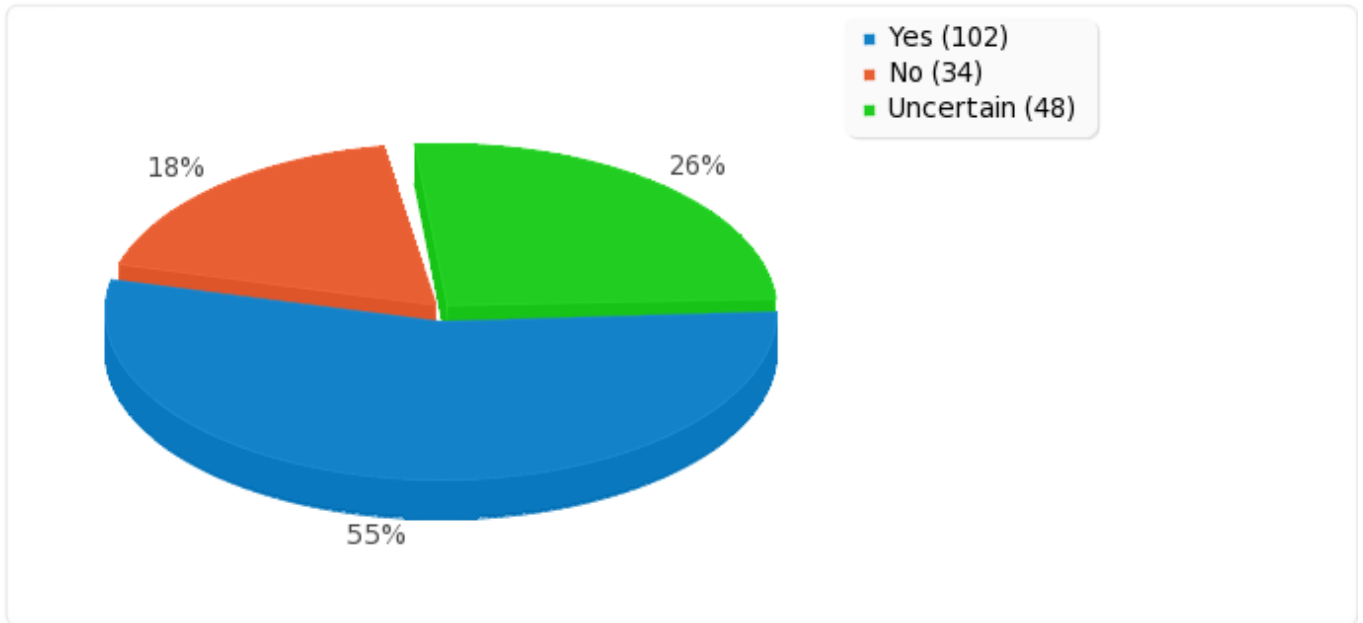
Answer	Count	Percentage
Yes (Y)	102	55.43%
No (N)	34	18.48%
Uncertain (U)	48	26.09%
No answer	0	0.00%



Field summary for reduceConcern(law)

Would the following measures help in reducing user concerns about privacy?  
[Privacy Laws - Describing which national law the system is compliant with  
(e.g., HIPAA in the US, European privacy laws)]

---





---

Field summary for reduceConcern(anon)

Would the following measures help in reducing user concerns about privacy?  
[Anonymizing all data  Ensuring that none of the data has any personal  
identifiers]

---

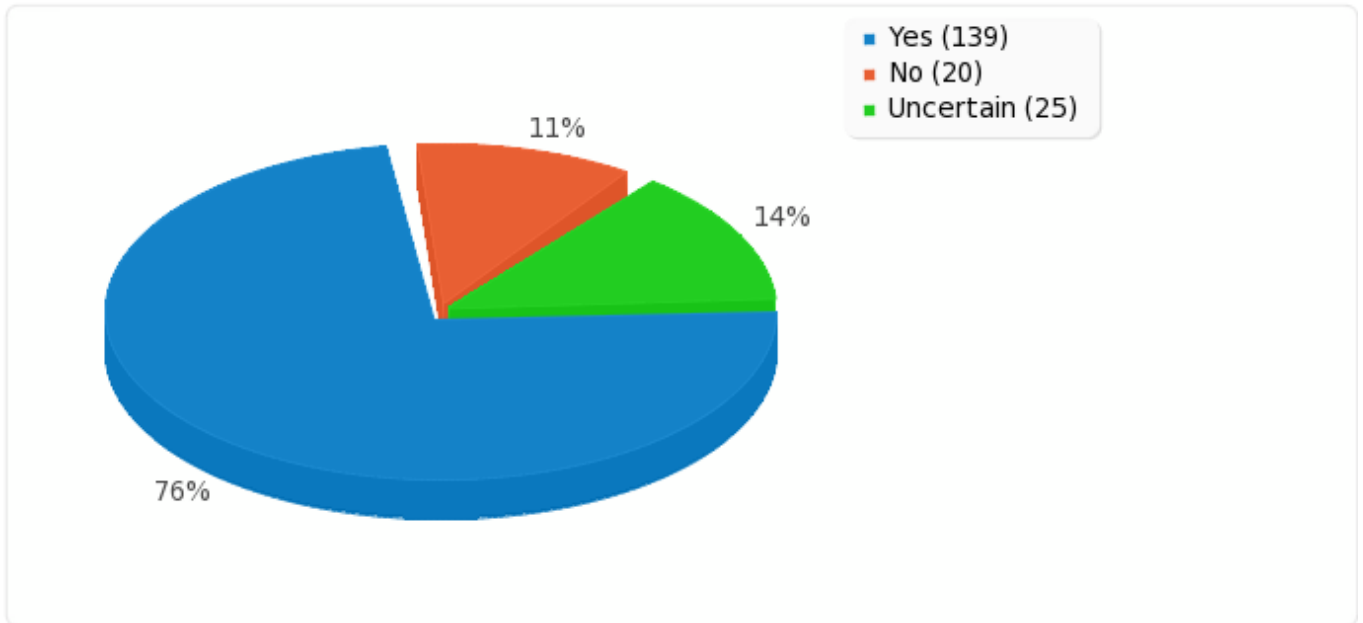
Answer	Count	Percentage
Yes (Y)	139	75.54%
No (N)	20	10.87%
Uncertain (U)	25	13.59%
No answer	0	0.00%



Field summary for reduceConcern(anon)

Would the following measures help in reducing user concerns about privacy?  
[Anonymizing all data - Ensuring that none of the data has any personal identifiers]

---





---

Field summary for reduceConcern(check)

Would the following measures help in reducing user concerns about privacy?  
[Please select "Yes " for this row]

---

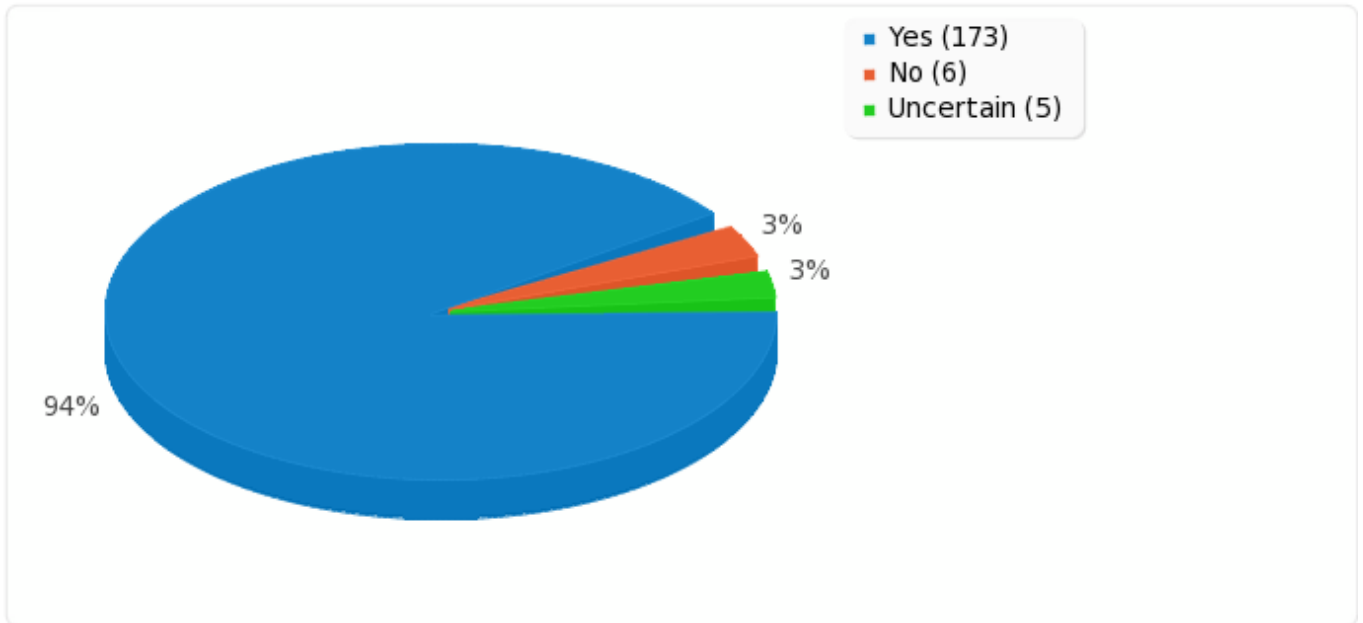
Answer	Count	Percentage
Yes (Y)	173	94.02%
No (N)	6	3.26%
Uncertain (U)	5	2.72%
No answer	0	0.00%



Field summary for reduceConcern(check)

Would the following measures help in reducing user concerns about privacy?  
[Please select "Yes " for this row]

---





---

Field summary for reduceConcern(tech)

Would the following measures help in reducing user concerns about privacy?  
[Technical Details [Describing the algorithms/source code of the system in order to achieve higher trust (E.g., encryption of data)]]

---

Answer	Count	Percentage
Yes (Y)	67	36.41%
No (N)	57	30.98%
Uncertain (U)	60	32.61%
No answer	0	0.00%

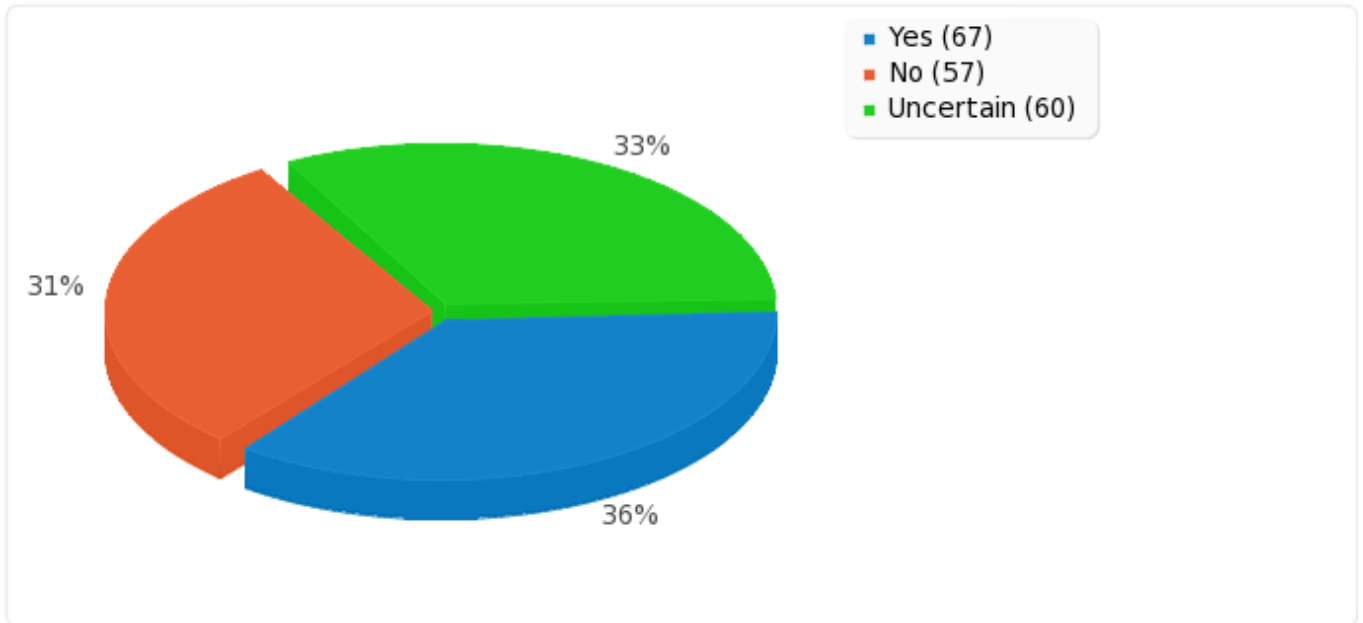




Field summary for reduceConcern(tech)

Would the following measures help in reducing user concerns about privacy?  
[Technical Details [Describing the algorithms/source code of the system in order to achieve higher trust (E.g., encryption of data)]]

---





---

Field summary for reduceConcern(usage)

Would the following measures help in reducing user concerns about privacy?  
[Details on usage [Describe, e.g., in a table how different data are used]

---

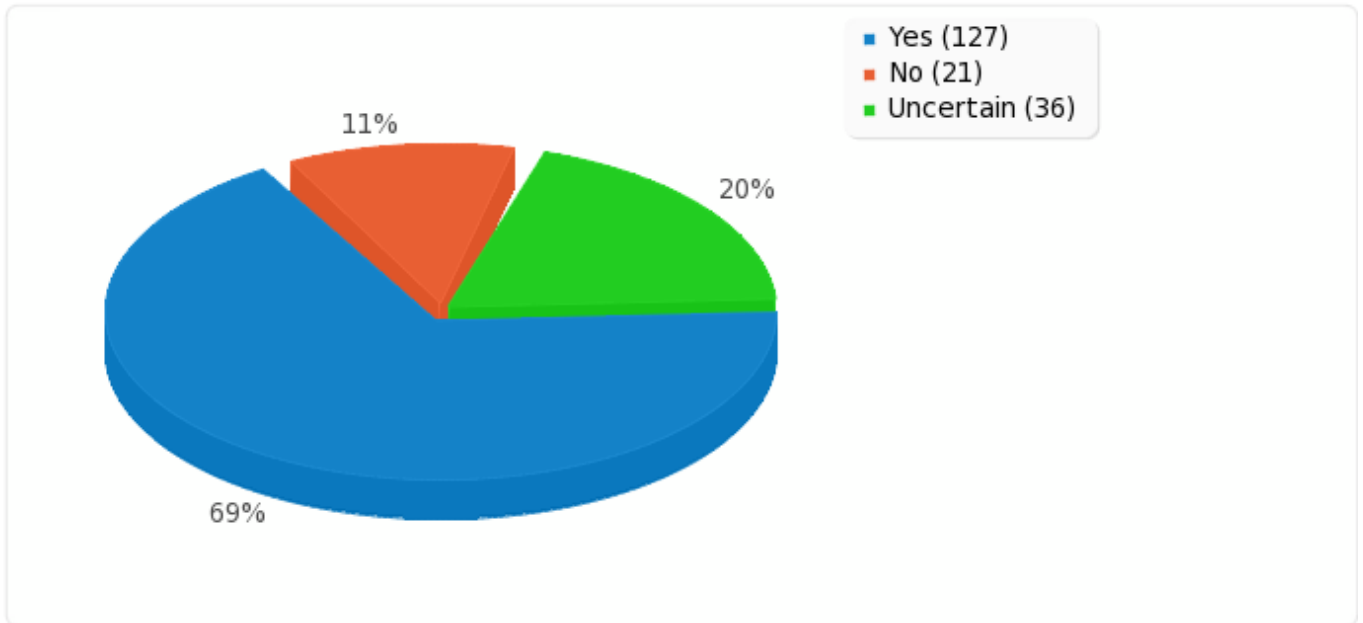
Answer	Count	Percentage
Yes (Y)	127	69.02%
No (N)	21	11.41%
Uncertain (U)	36	19.57%
No answer	0	0.00%



Field summary for reduceConcern(usage)

Would the following measures help in reducing user concerns about privacy?  
[Details on usage ¶Describe, e.g., in a table how different data are used]

---





## Field summary for UadditionalReduce

Are there additional measures to reduce concerns about privacy? Why?

Answer	Count	Percentage
Answer	16	17.20%
No answer	77	82.80%

**Responses**

No

Ich glaube, dass es in Zukunft sehr schwer sein wird, die Bedenken der Nutzer hinsichtlich des Datenschutzes zu zerstreuen, wenn die NSA und andere Geheimdienste auf Firmendaten und das "freie" Internet ohne richterlichen Beschluss zu greifen können.

An label that indicates that the company successfully had a privacy audit by an independent party. I don't believe what companies say they do, I want proof!

v.a. Datenschutzgesetze sind zentral

Zusammenarbeit mit der nationalen Regierung, Erreichbarkeit bei Nachfragen, einfach Möglichkeiten Daten als User zu löschen und zwar komplett (zumindest auf der jeweiligen Plattform)

Aufklärung, wie mitunter Datenmissbrauch betrieben wird und wie man in einem solchen Fall dagegen vorgehen könnte.

Mitteilung, an wen, welche Daten übermittelt werden

Reputation - Vertraut man einem System, einer Institution oder Firma fällt es leichter auch sensible Daten preiszugeben. Die Datenlecks in der Vergangenheit (Telekom, CH-Steuerhinterzieher-CDs etc.) und die aktuelle Diskussion (Prism, Google & Co als "Zulieferer" für Geheimdienste) werden jedoch diesen Ansatz weiter erschweren  
Don't store data, design a truly unbreakable password system

Ersichtlichkeit, dass das Datensammeln nicht mit der Hauptzweck und nicht mit die Haupteinnahmequelle einer Einrichtung ist.

Die versicherung Versicherung dass daten nach der nötigen Benutzung wieder gelöscht werden.

rechtliche regelungen, die dem benutzer jederzeit erlauben einsicht zu nehmen in die menge an daten, die ein dienstanbieter vorhälte klare verbote der datenweitergabe, ohne vorherige zustimmung bei verstößen gegen bestimmungen, empfindliche geldstrafen bis zu einstellung des geschäftsbetriebs

löschmöglichkeiten im eigenen benutzerprofil, der benutzer kann seine daten immer wieder eigenhändig auf 0 setzen.

1. Eine zeitliche Limitierung der Speicherung (garantiertes Löschen aller bei einem System/ einer Website aggregierten Daten, z.B. alle 2-3 Jahre). 2. Offenlegung der Datenaggregation (z.B. bei Amazon: interessiert sich für x, y und z, kombiniert mit der Möglichkeit, Gespeichertes als Nutzer selbstbestimmt aus dem Profil zu löschen).

3. Das Anbieten eines stealth-modus, also z.B. bei einem Amazon-Kauf die Möglichkeit der Auswahl, ob der aktuelle Kauf im Profil gespeichert werden soll oder nicht (so dass man den Sommerlektüre-Krimi speichern lassen kann, den Dildo-Kauf jedoch nicht ;)

Möglichkeit der vollständigen Datenlöschung bei Abmeldung vom Dienst sofern keine gesetzlichen Vorgaben dem widersprechen.

2 Pc bzw Netzwerke eins ohne Internet für wichtige Daten! Relevante



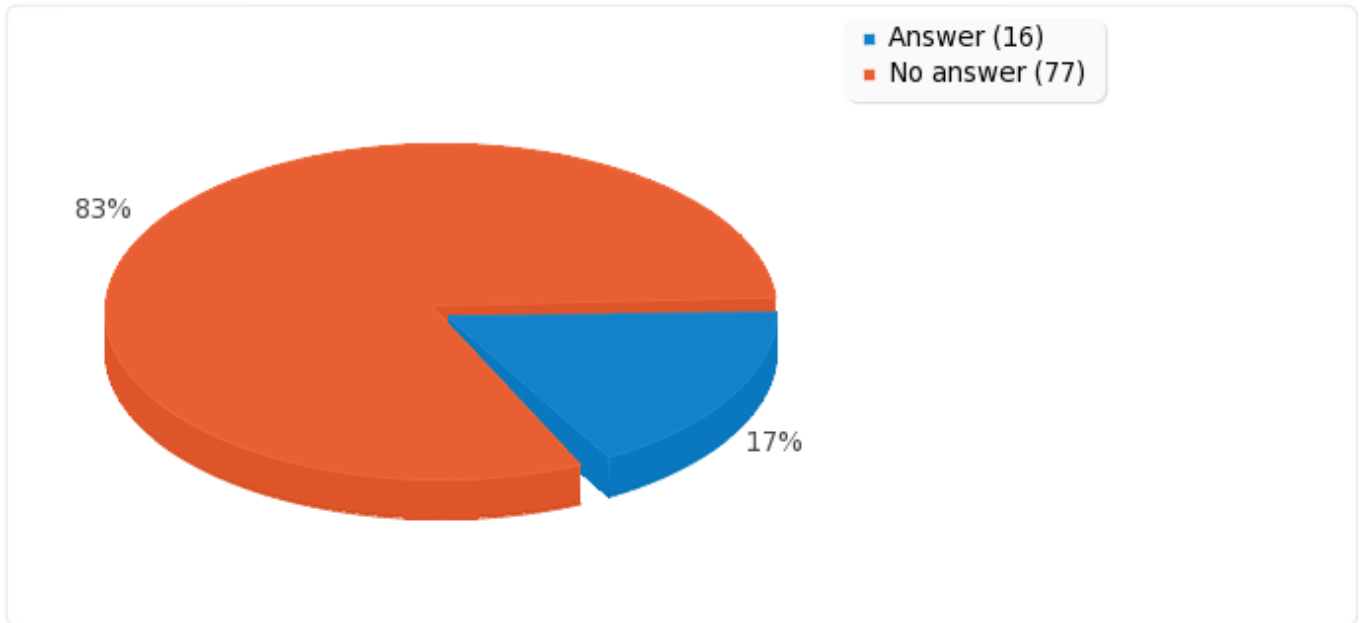
Daten nur per Kurier verschicken! Oder Post, die kann zwar auch  
gelesen werden ist aber schwieriger zu Speichern in der Masse.  
more transparancy and governmental control would be useful



Field summary for UadditionalReduce

Are there additional measures to reduce concerns about privacy? Why?

---





## Field summary for additionalReduce

Are there additional measures to reduce user concerns about privacy? Why?

Answer	Count	Percentage
Answer	42	22.83%
No answer	142	77.17%

**Responses**

control over data, the ability to remove personal data at will.

Überzeugende Arbeit des Anbieters in der Vergangenheit

Simple human readable assertions on what will and won't be done with data goes a long way. "We don't sell or share your dat

I think the main concern is that if you want to use a service, you are forced to agree to all of their terms of use; so if I want to use something like Instagram, I have to agree to let them 'own' my photos just to use the service. To alleviate privacy concerns, it should be possible to opt out of, or 'not agree' to certain terms.

- Datensparsamkeit (nur technisch notwendige Daten erheben, keine Speicherung von IP-Adressen über eine Sitzung/Session hinaus)

- Opt-In-Verfahren für alle zusätzlichen Datensammelfunktionen mit Disclaimer: "Wenn Sie diese Funktion nutzen, werden folgende Daten erhoben und so und so gespeichert und für diese Zwecke verwendet."

Der Disclaimer muss direkt im User-Interface bei der Auswahlmöglichkeit stehen und nicht in den AGB versteckt sein.

Wenn die technischen Details (Beschreibung der Algorithmen etc.) von unabhängigen Experten begutachtet werden und deren Urteil dann knapp und übersichtlich präsentiert öffentlich wird.

it is important to have good policies about deleting your account / info. i.e. a user should be able to say "I want you to delete all the info you have about me" and know that the company will comply.

No

Policies / EULA might not matter as many might not read it. Only becomes relevant when someone calls out specifics, e.g. in a blog post that gets much attention.

Note: "less privacy" below is too blurry to say yes or no.

Making your source code publicly available shall almost surely eliminate the most common privacy concerns.

Transparenz und Datenminimierung - wie vom Datenschutz allgemein gefordert.

Den Nutzern ist der Datenschutz egal oder die beschriebenen Punkte werden nicht verstanden. Insofern ist auch jeder Versuch, die Bedenken zu zerstreuen, sinnlos. Es sind einfach keinerlei Bedenken da. Facebook, Payback-Karte ertc. werden benutzt, ohne über die Fubnktion nachzudenken. Hier muss angesetzt werden: Es muss über die Problematik informiert werden.

Begründung für Abfrage bestimmter Daten/Attribute; OPT-IN statt OPT-OUT; Ein/Ausschluss bestimmter Attribute

Verminderung der erhobenen / gespeicherten Datenmenge, Ermöglichung eines anonymen Zugangs

Kurze, verständliche AGBs, keine seitenlange Juristensprache.

Zu Nutzungsdetails: JA nur, wenn man mit den Angaben einverstanden ist und einen Mehrwert dahinter sieht.



Siegel wie SaferShopping, TÜV, etc.

Improve Anonymizing all data

Ensuring that none of the data has any personal identifiers, but also that cannot be further processed in order to stop data mining the data.

Zertifikate von "unabhängigen" Dritten

Test-Vergleiche in den Medien

Neben technischen Details könnte man auch Aussagen darüber machen, wie mit Incidents umgegangen wird.

Datenschutzbedenken werden beim Durchschnittsnutzer in erster Linie dadurch zerstreut, dass seine Aufmerksamkeit so wenig wie möglich auf Datenschutz und die Datenschutzproblematiken gerichtet werden.

Ein weiteres---etwas ehrlicheres---Mittel gegen Datenschutzbedenken ist die aktive Gestaltung des Auftretens als rundherum vertrauenswürdiger Dienst.

If encryption is done, it should always be using open-source algorithms. It has been proven time and time again that proprietary algorithms are by default more insecure because they cannot be analyzed and tested by a wide range of professionals.

Maybe an extreme measure, but something that would reduce my concerns would be to show me an example of the data that is sent by a particular application. e.g. WhatsApp wants to send data over the Internet. This is what we send: . In nowadays world with NSA and everything, I find this is more than ever a necessity.

Anonymes Agieren auf der Webseite

shut down prism?

End Point Verschlüsselung

Have a short data retention period.

Conduct third-party audits and share their findings.

Allow users to access to a summary of all the data stored on their behalf, and allow them to delete all or part of it if they desire.

Ensure to user be able to control their information as flexible as possible. And make them choose the degree of privacy.

I am not sure users will be much interested in the last point. But perhaps, having it public opens the door to discussing it in forums by experts in a way visible to "normal" users so their level of trust increases (or decreases, depends on what experts say).

By he way, the questions are becoming unclear whether you mean users or programmers..

Also,why did you ask the participants to say Yes above :)

With regards to Question about "how critical".. the third item, it is unclear whether it collects also the content on which the mouse is or only its coordination.

Perhaps for the user to be able to delete all (or part of) their data at any time.

For the system to never see the user data "in the clear".

Eine grundlegende Transparenz ist zwar wünschenswert aber würde in den meisten Fällen vermutlich doch ungelesen am großteil der Nutzer vorbeiziehen. Trotzdem wäre sie wünschenswert, da sich dann unabhängige Experten wie der CCC oder ähnlich Gruppen intensiver mit einzelnen Firmen auseinander setzen könnten. Ob sie allerdings die tatsächliche Transparenz die gefühlte Transparenz beim Nutzer allerdings stark beeinflussen kann, darf glaube ich bezweifelt werden.

Describing physical safety measures of servers (i.e., how the





actual servers the data is stored on are physically locked away), possibly qualifications of people handling data and what they have access to under which circumstances, how long the data is stored before it is erased

Anonymization is the only way that I think is acceptable.

Building a reputation for preserving privacy. Hiring famous cryptographers, challenging government requests in courts etc.

Es gibt leider keinen Ansatz, weil kein System nur laut einer Aussage glaubhaft machen kann, dass Daten nicht abgegriffen werden. Wenn nicht vom System selber, dann halt durch System, die von diesem System benutzt werden.

Des weiteren ist ja auch bekannt, dass alle Systeme grundsätzlich ein Sicherheits-Limit haben (z.B. 2048 Bit PGP), dass auf jeden Fall noch durch Geheimdienste entschlüsselt werden kann. Also macht das alles aus Datenschutzgründen keinen Sinn.

Selbst das ablegen der Daten auf dem eigenen Rechner ist schließlich schon ein Problem, weil selbst diese ausgespäht werden. Erst recht dann Datenbanken.

Eigentlich muss das (langfristige) Sammeln von Daten in Datenbanken grundsätzlich verboten werden, weil diese genau dieses Problem machen.

Not allowing users data being stored in servers. Just maintaining them in the source.

- Allowing fine grained control over sharing options, using a well documented interface.

- Warning of sharing by default options.

Use of data should be explained in a simple language, and short text. Privacy policies should be written in a short way and simpler language.

Transparency: Giving the user access to the stored data to browse it herself.

no

of course:

- Giving the users the freedom to choose what data they share.

- having a "privacy police" to check on how data is handled

- more tools to protect online privacy

- educating users about privacy

Die gegebenen Daten sollten nur für jeweils eine kleine überschaubare Aufgabe verwendet werden - die Weitergabe an andere Instanzen sollte entweder vermieden werden, oder es sollte direkt und deutlich drauf hingewiesen werden, an wen die Daten warum weitergegeben werden.

Für einige Datensammlungen (wie soziale Netzwerke) dürfte es keine Pflicht geben, den Realnamen anzugeben.

Ein staatliches Zertifikat, welches den Datenschutz überprüft und eine staatliche Datenbank mit solchen Seiten, um die Fälschung solcher Zertifikate zu verhindern.

Datensparsamkeit

Trennung von Daten

Aktive Löschmöglichkeit

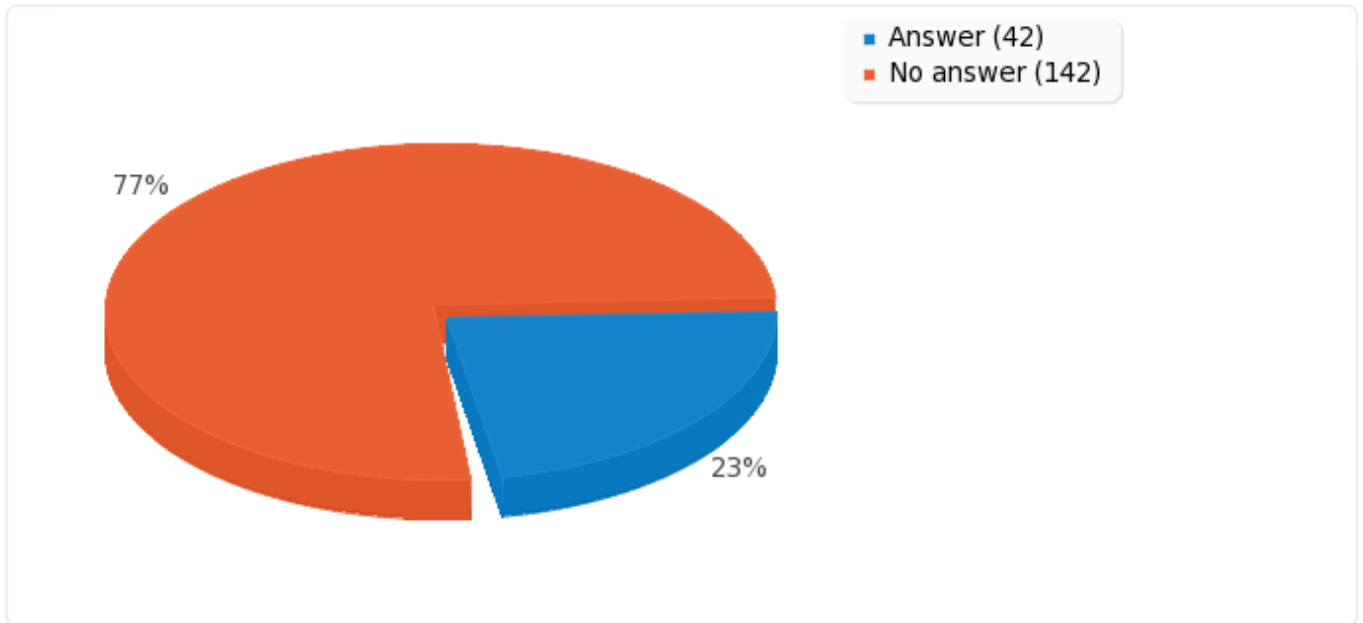
Zertifizierung der Systeme durch dritte ( e.g. Privacy Audit, Security Audit, etc..)



Field summary for additionalReduce

Are there additional measures to reduce user concerns about privacy? Why?

---





---

Field summary for Q00111

What information about users should systems never capture ? Why?

---

Answer	Count	Percentage
Answer	0	0.00%
No answer	184	100.00%

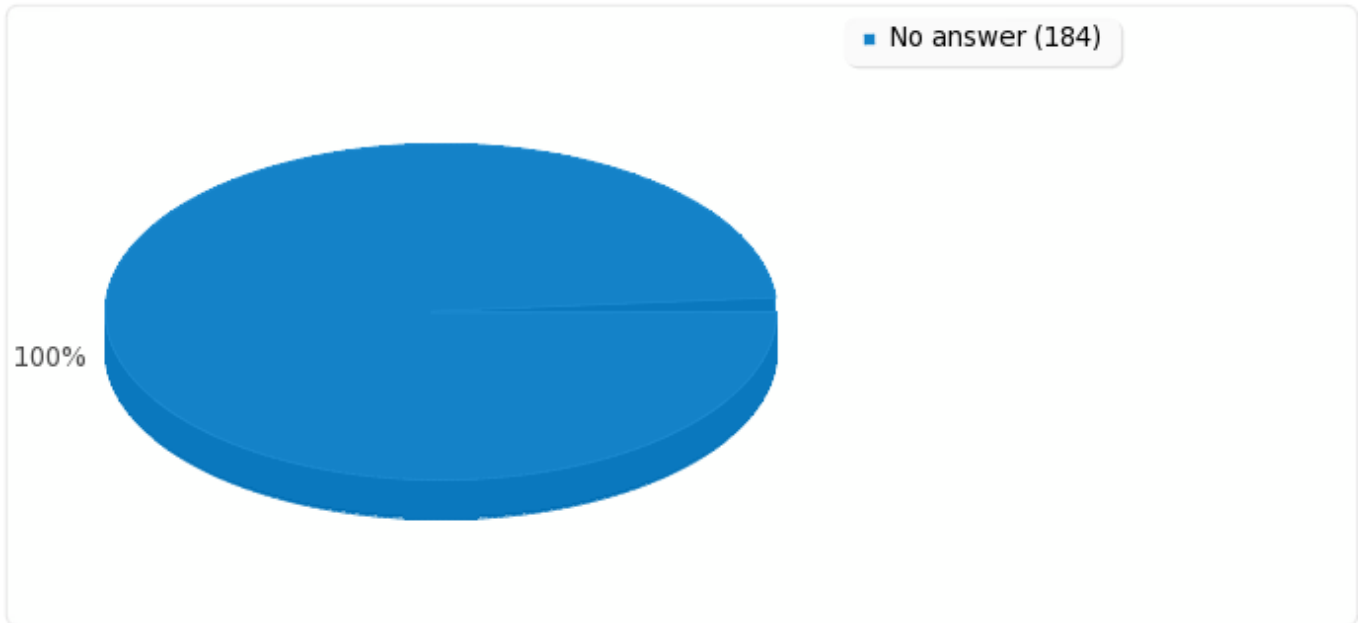
**Responses**



Field summary for Q00111

What information about users should systems never capture ? Why?

---





---

Field summary for lessPrivacy(func)

Would you accept less privacy for the following?  
["Intelligent" or additional functionality of the system (such as the Amazon recommendations)]

---

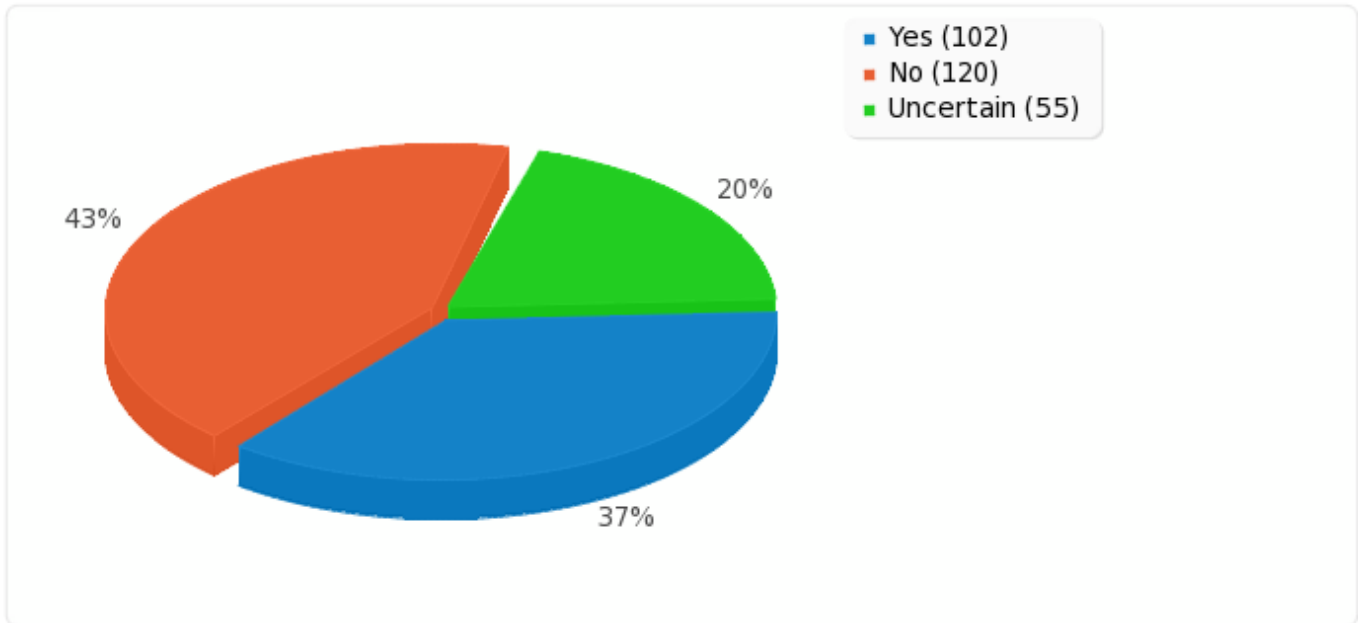
Answer	Count	Percentage
Yes (Y)	102	36.82%
No (N)	120	43.32%
Uncertain (U)	55	19.86%
No answer	0	0.00%



Field summary for lessPrivacy(func)

Would you accept less privacy for the following?  
["Intelligent" or additional functionality of the system (such as the Amazon recommendations)]

---





---

Field summary for lessPrivacy(ad)

Would you accept less privacy for the following?  
[Fewer advertisements]

---

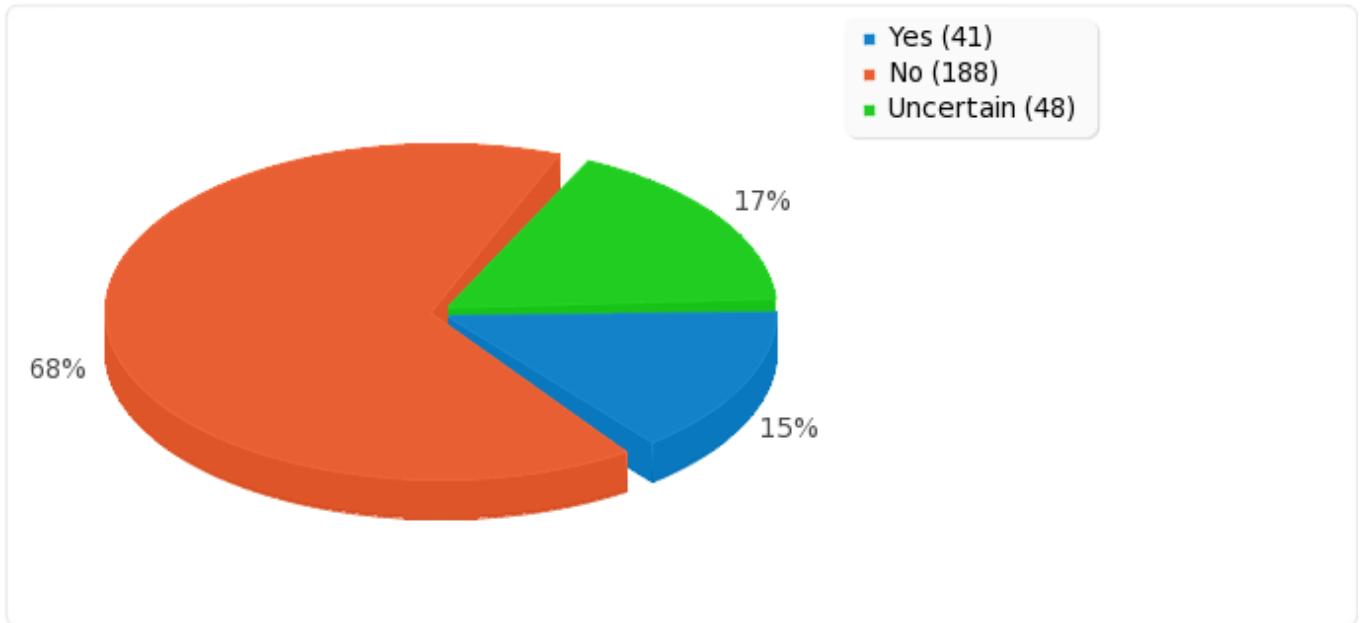
Answer	Count	Percentage
Yes (Y)	41	14.80%
No (N)	188	67.87%
Uncertain (U)	48	17.33%
No answer	0	0.00%



Field summary for lessPrivacy(ad)

Would you accept less privacy for the following?  
[Fewer advertisements]

---







---

Field summary for lessPrivacy(money)

Would you accept less privacy for the following?  
[Monetary discounts (e.g., 10% discount on the next purchase)]

---

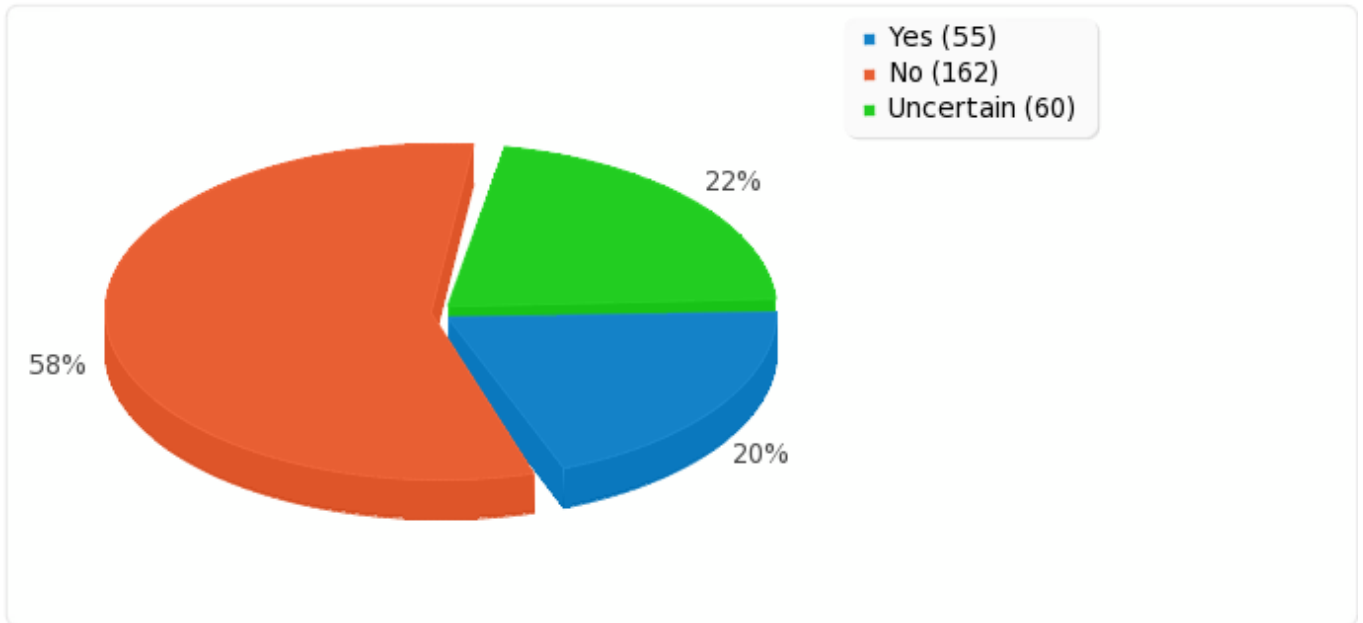
Answer	Count	Percentage
Yes (Y)	55	19.86%
No (N)	162	58.48%
Uncertain (U)	60	21.66%
No answer	0	0.00%



Field summary for lessPrivacy(money)

Would you accept less privacy for the following?  
[Monetary discounts (e.g., 10% discount on the next purchase)]

---





---

Field summary for privacyCriticality(conten)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Content of documents (such as the email body)]

---

Answer	Count	Percentage	Sum
1 (1)	204	73.65%	91.70%
2 (2)	50	18.05%	
3 (3)	9	3.25%	3.25%
4 (4)	8	2.89%	
5 (5)	6	2.17%	5.05%
No answer	0	0.00%	
Arithmetic mean	1.42		
Standard deviation	0.86		
Sum (Answers)	277	100.00%	100.00%
Number of cases	277	100.00%	



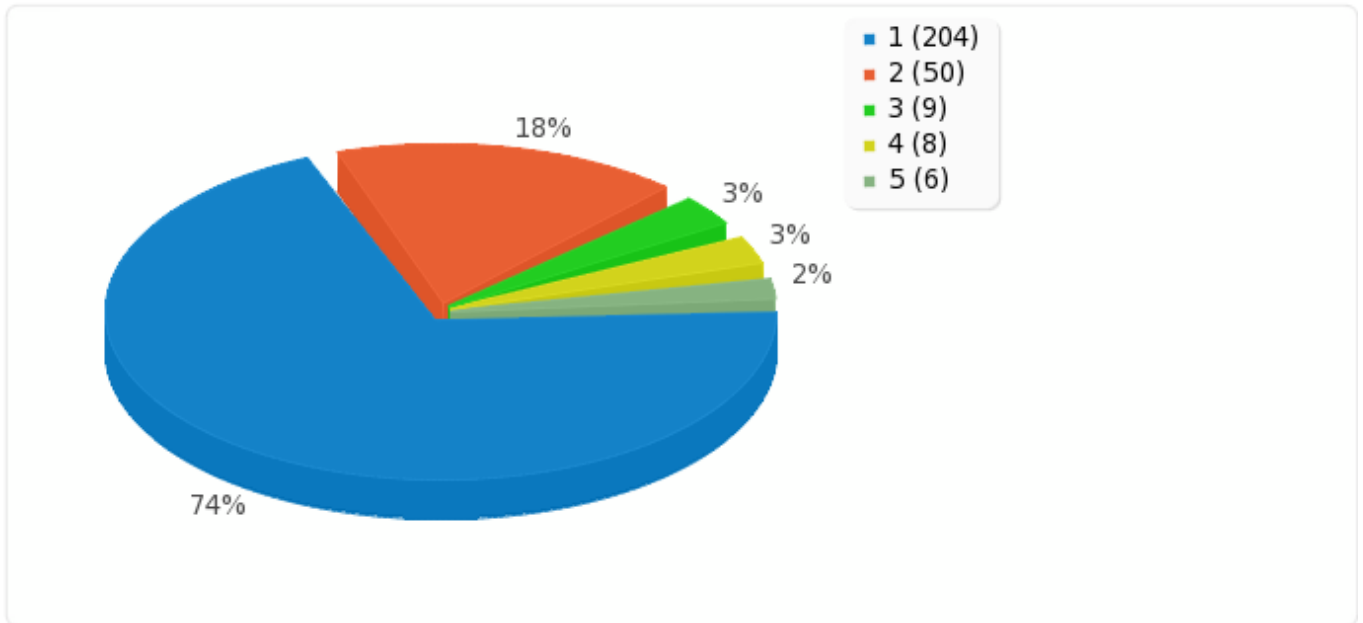
Field summary for privacyCriticality(conte)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Content of documents (such as the email body)]

---





---

Field summary for privacyCriticality(meta)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Metadata (such as date)]

---

Answer	Count	Percentage	Sum
1 (1)	36	13.00%	50.18%
2 (2)	103	37.18%	
3 (3)	76	27.44%	27.44%
4 (4)	44	15.88%	
5 (5)	18	6.50%	22.38%
No answer	0	0.00%	
Arithmetic mean	2.66		
Standard deviation	1.09		
Sum (Answers)	277	100.00%	100.00%
Number of cases	277	100.00%	

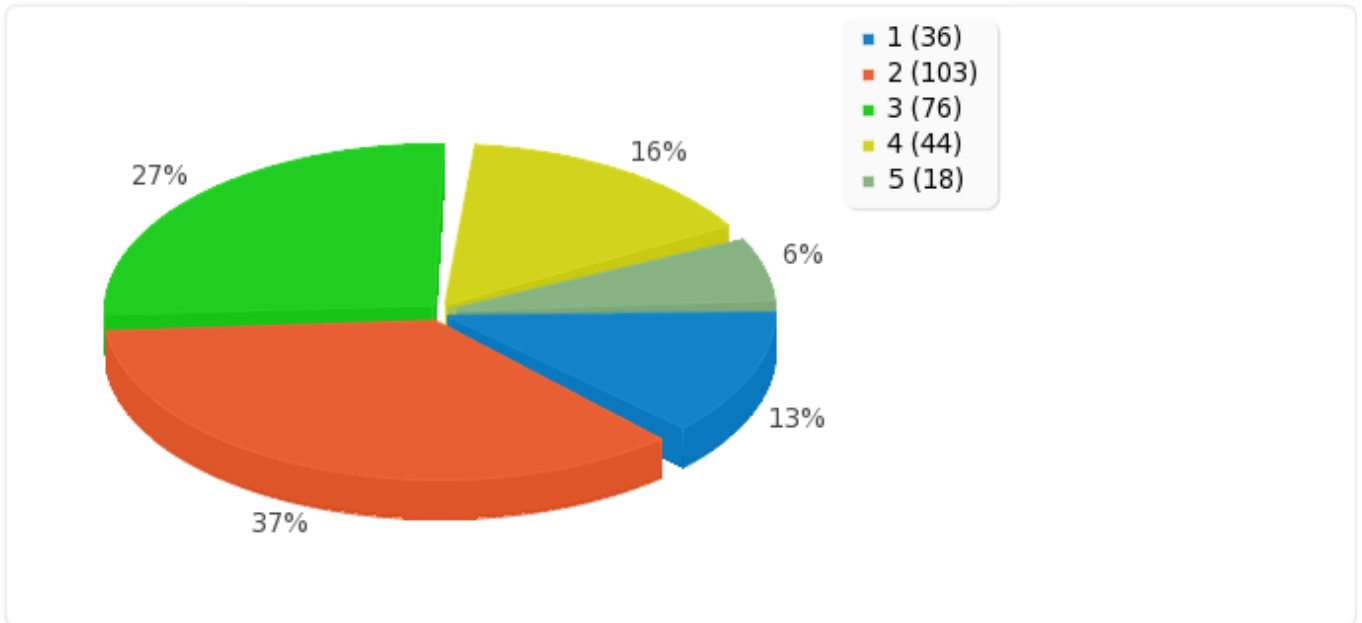


Field summary for privacyCriticality(meta)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Metadata (such as date)]





---

Field summary for privacyCriticality(inter)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Interaction (such as a mouse click to open or send an email)]

---

Answer	Count	Percentage	Sum
1 (1)	66	23.83%	57.76%
2 (2)	94	33.94%	
3 (3)	68	24.55%	24.55%
4 (4)	36	13.00%	
5 (5)	13	4.69%	17.69%
No answer	0	0.00%	
Arithmetic mean	2.41		
Standard deviation	1.12		
Sum (Answers)	277	100.00%	100.00%
Number of cases	277	100.00%	



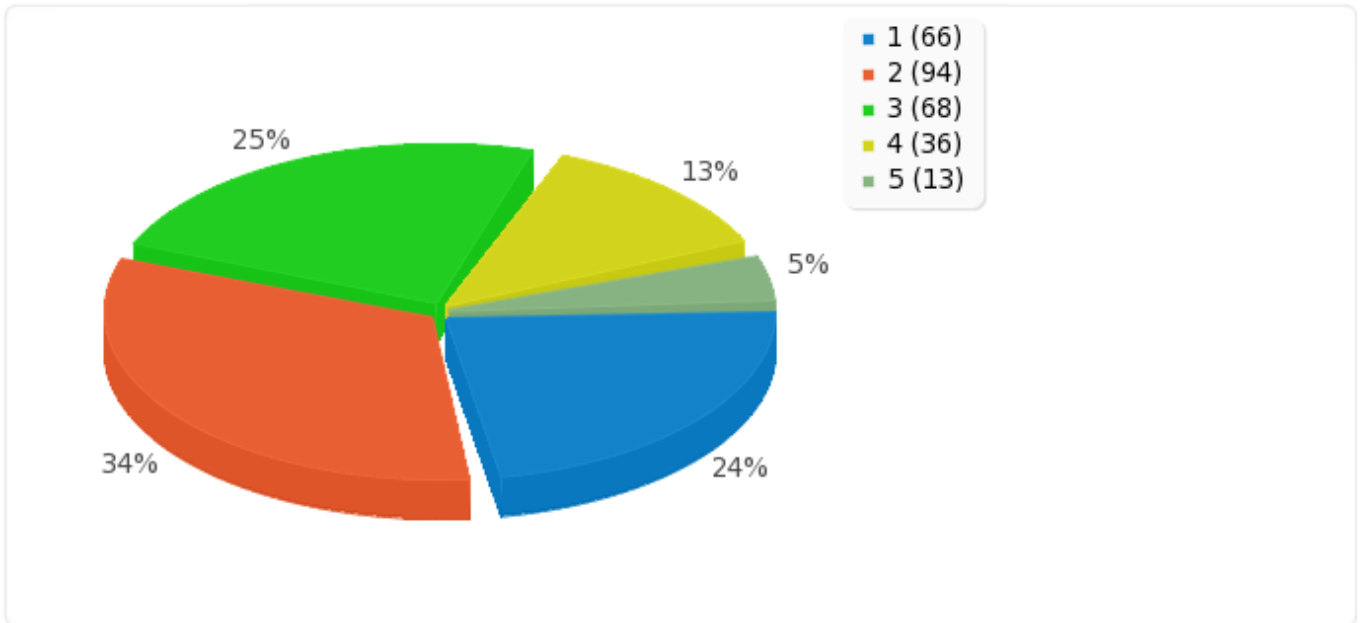
Field summary for privacyCriticality(inter)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Interaction (such as a mouse click to open or send an email)]

---







---

Field summary for privacyCriticality(loc)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[User location]

---

Answer	Count	Percentage	Sum
1 (1)	138	49.82%	83.39%
2 (2)	93	33.57%	
3 (3)	24	8.66%	8.66%
4 (4)	13	4.69%	
5 (5)	9	3.25%	7.94%
No answer	0	0.00%	
Arithmetic mean	1.78		
Standard deviation	1.01		
Sum (Answers)	277	100.00%	100.00%
Number of cases	277	100.00%	

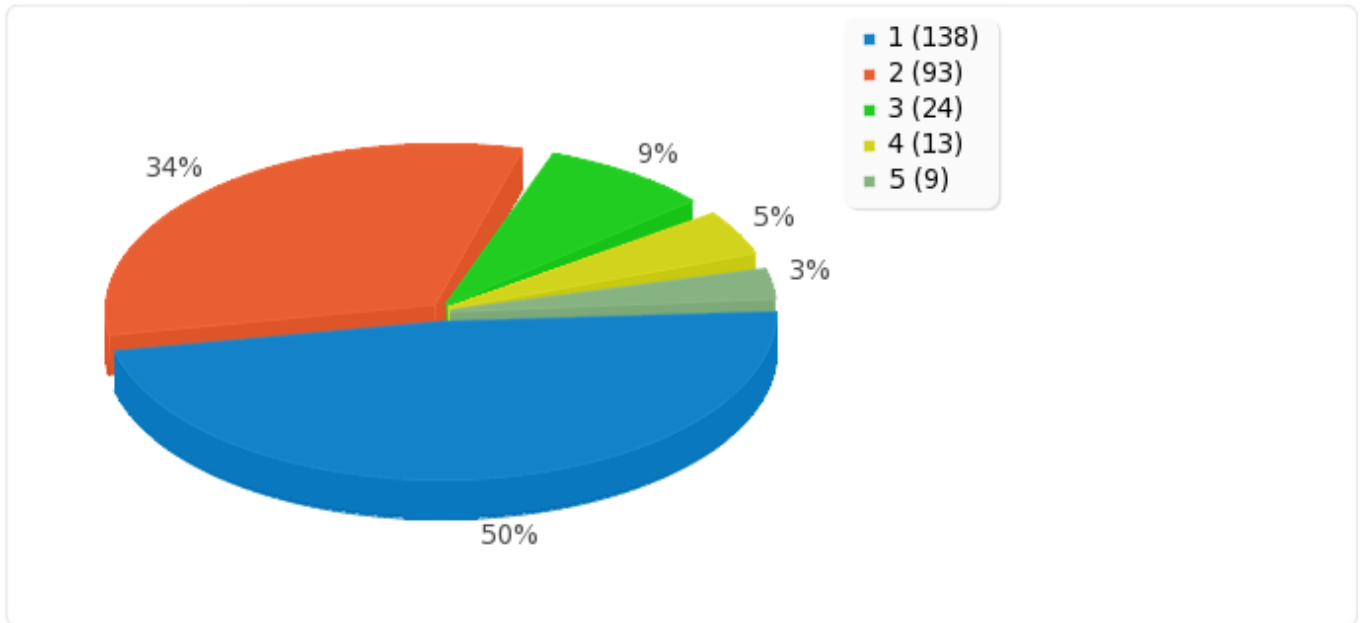


Field summary for privacyCriticality(loc)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[User location]





Field summary for privacyCriticality(name)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Name or personal data]

Answer	Count	Percentage	Sum
1 (1)	204	73.65%	88.81%
2 (2)	42	15.16%	
3 (3)	12	4.33%	4.33%
4 (4)	9	3.25%	
5 (5)	10	3.61%	6.86%
No answer	0	0.00%	
Arithmetic mean	1.48		
Standard deviation	0.98		
Sum (Answers)	277	100.00%	100.00%
Number of cases	277	100.00%	

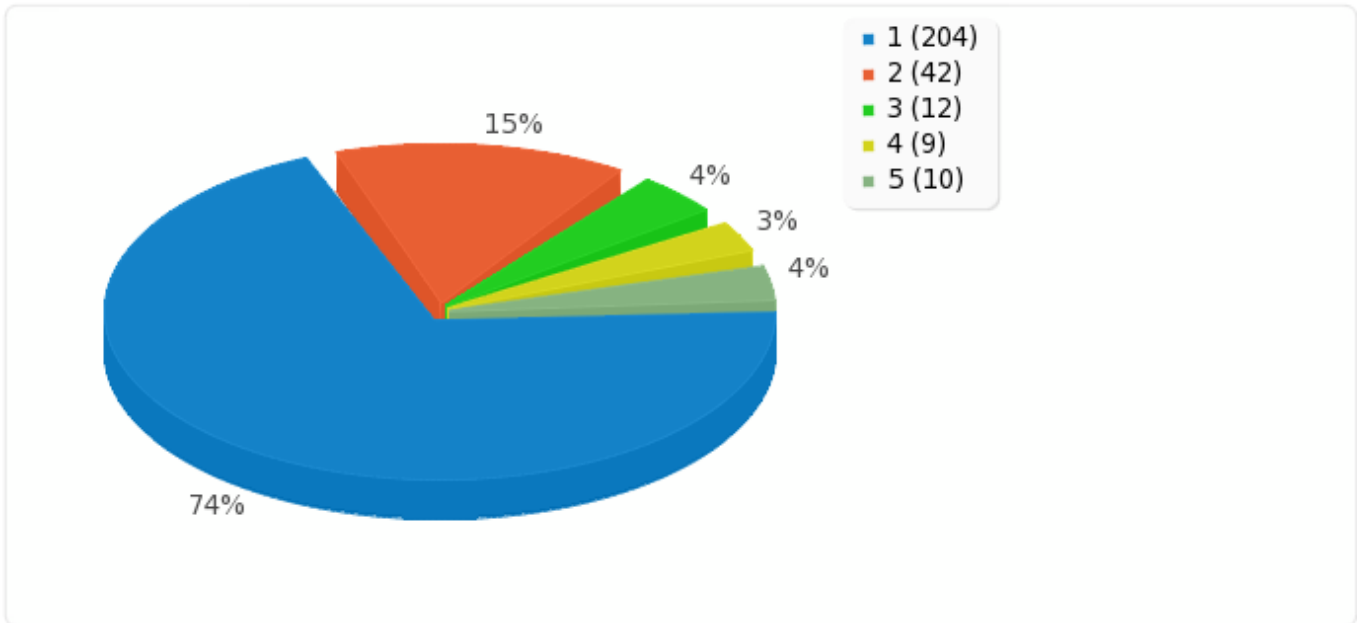


Field summary for privacyCriticality(name)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[Name or personal data]





---

Field summary for privacyCriticality(pref)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[User preferences]

---

Answer	Count	Percentage	Sum
1 (1)	105	37.91%	69.68%
2 (2)	88	31.77%	
3 (3)	53	19.13%	19.13%
4 (4)	21	7.58%	
5 (5)	10	3.61%	11.19%
No answer	0	0.00%	
Arithmetic mean	2.07		
Standard deviation	1.09		
Sum (Answers)	277	100.00%	100.00%
Number of cases	277	100.00%	

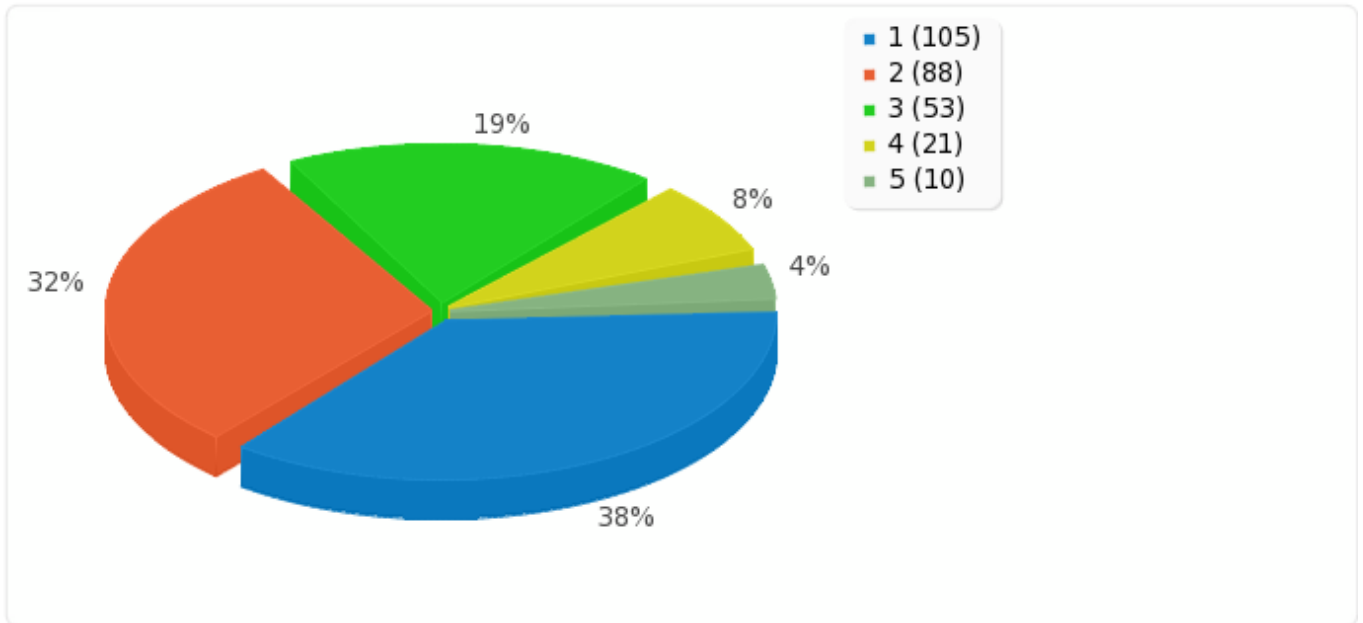


Field summary for privacyCriticality(pref)

How critical would you rate the collection of the following data?

(1 - very critical, 2 - critical, 3 - neutral, 4 - somewhat uncritical, 5 - uncritical)

[User preferences]





---

Field summary for affiliation

What is your affiliation?

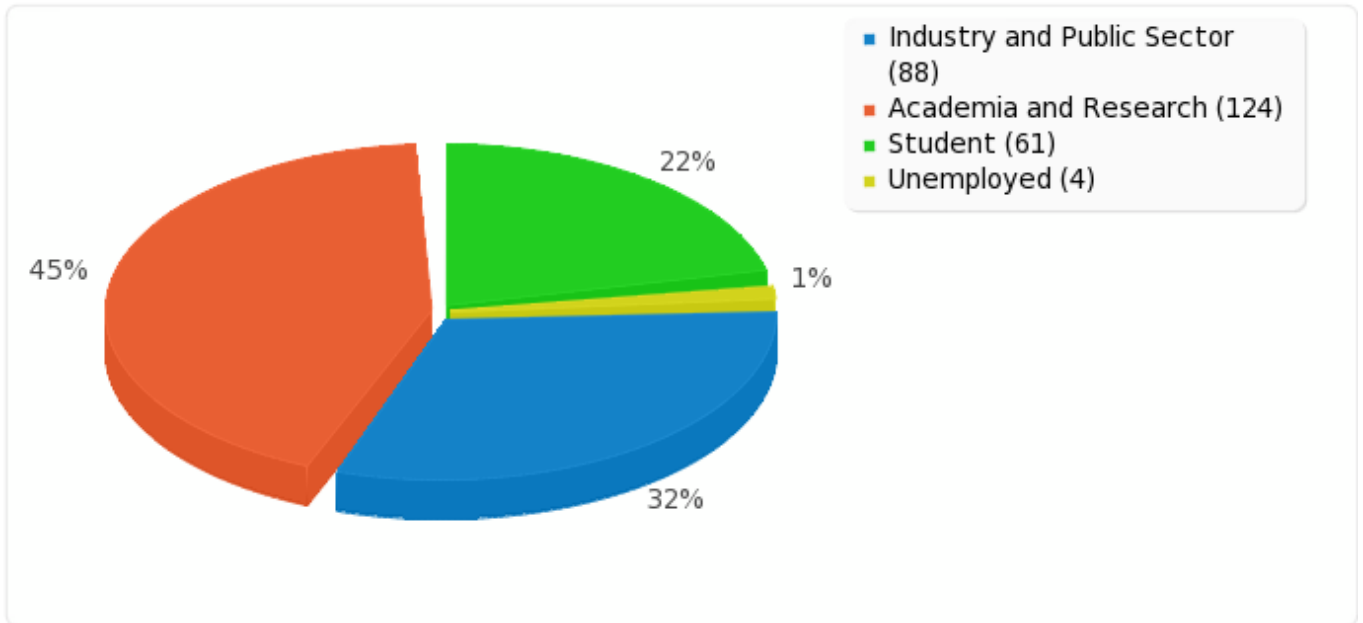
---

Answer	Count	Percentage
Industry and Public Sector (ind)	88	31.77%
Academia and Research (acad)	124	44.77%
Student (stud)	61	22.02%
Unemployed (un)	4	1.44%
No answer	0	0.00%



Field summary for affiliation

What is your affiliation?







---

Field summary for Q0023

In which continent have you primarily lived in the last few years?

---

Answer	Count	Percentage
North America (SQ001)	0	0.00%
South America (SQ002)	0	0.00%
Europe (SQ003)	0	0.00%
Asia (SQ004)	0	0.00%
Africa (SQ005)	0	0.00%
Other	0	0.00%

**Other Responses**



---

Field summary for live

Where do you live?

---

Answer	Count	Percentage
North America (na)	72	25.99%
South America (sa)	3	1.08%
Europe (e)	191	68.95%
Asia/Pacific (ap)	6	2.17%
Africa (af)	2	0.72%
Other	2	0.72%
No answer	0	0.00%

**Other Responses**

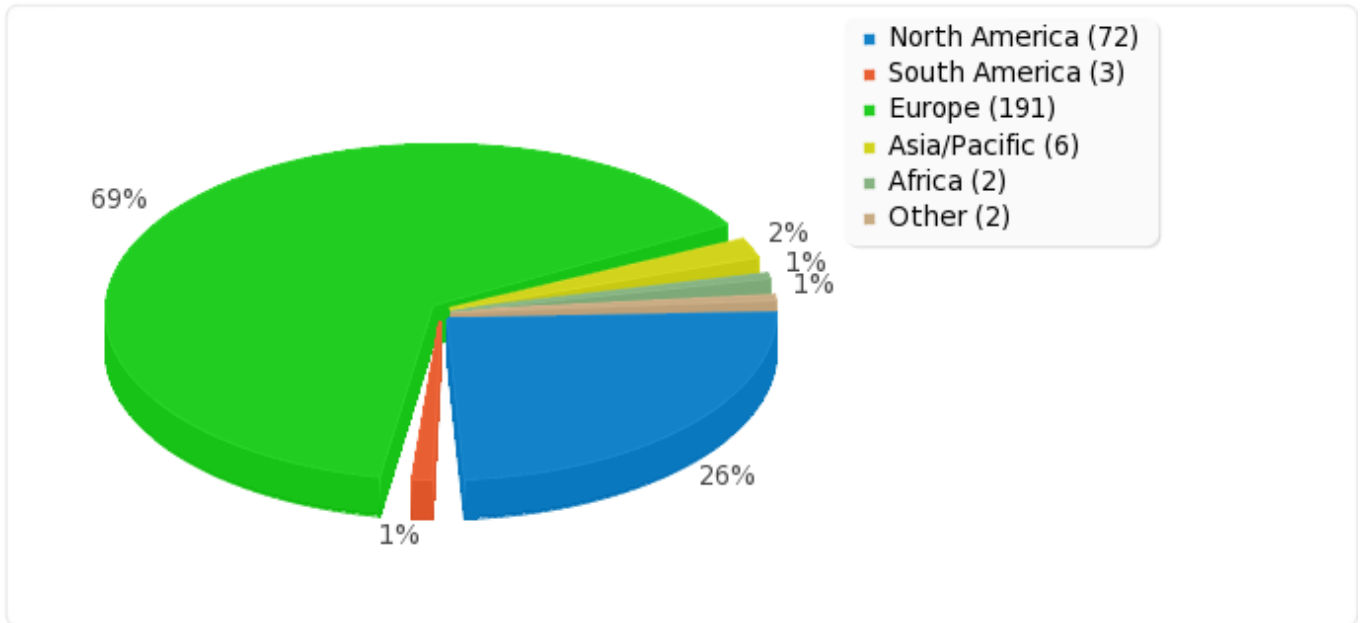
other

Jordan



Field summary for live

Where do you live?





Field summary for identify

With which region do you identify yourself?

Answer	Count	Percentage
North America (na)	55	19.86%
South America (sa)	5	1.81%
Europe (e)	192	69.31%
Asia/Pacific (ap)	15	5.42%
Africa (af)	4	1.44%
Other	5	1.81%
No answer	0	0.00%

**Other Responses**

Australien

Bayern

Middle Eastern

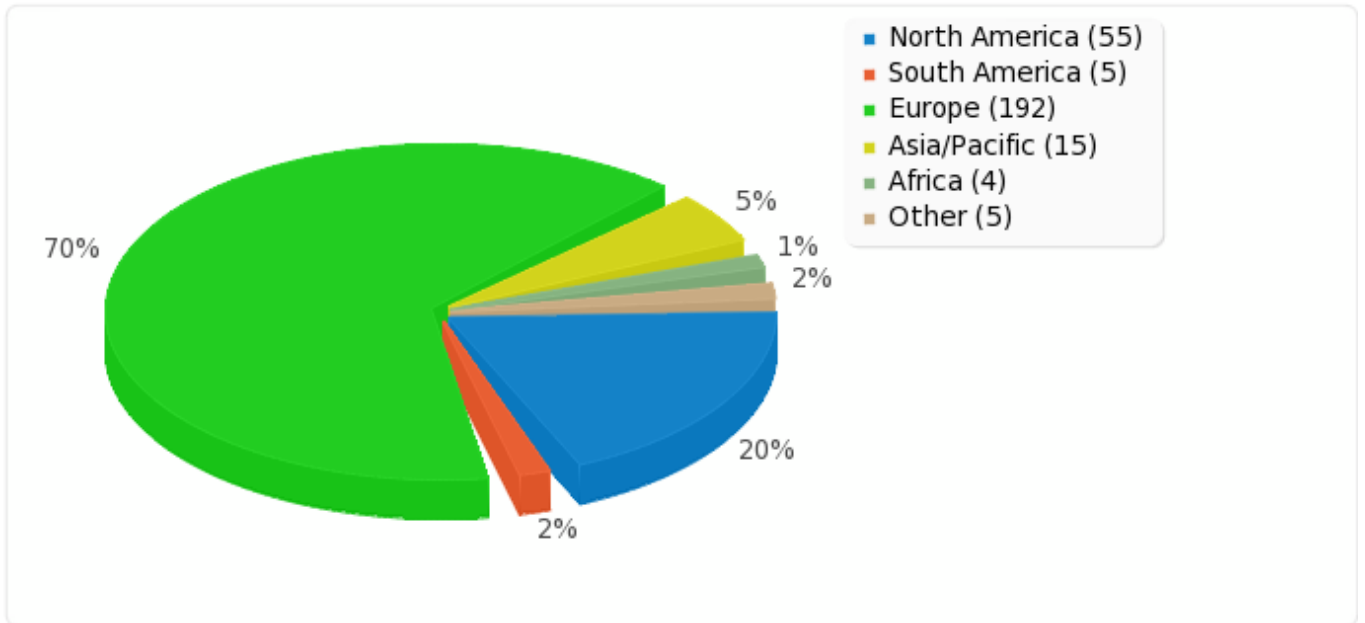
non western 'homogeneous' hamburger countries (Latin America, East, Asia, Africa)

Jordan



Field summary for identify

With which region do you identify yourself?





---

Field summary for check2

What is the sum of 2 and 5?

---

Calculation	Result
Count	277
Sum	1995
Standard deviation	2.36
Average	7.2
Minimum	7
1st quartile (Q1)	7
Median value	7
3rd quartile (Q3)	7
Maximum	42

**Null values are ignored in calculations**  
**Q1 and Q3 calculated using minitab method**