Understanding the Right to be Forgotten and its Deployment

Jianbing Ni, Xiangman Li, Eric Li, and Jianxiang Zhao

Queen's University, Kingston, ON

Ubiquitous data collection poses severe risks of privacy leakage to customers accessing various web services in the connected world. Due to frequent data breach incidents, the regulation of data collection and usage has garnered significant attention, leading to the issuance of various privacy laws aimed at promoting personal data protection. However, data deletion, a critical aspect of ensuring the closure of the data lifecycle, is often neglected. GDPR Article 17 [1] introduces the right to erasure, also known as the right to be forgotten, granting data subjects (i.e., customers) the right to request the deletion of their personal data held by service providers, such as government entities, tech giants, or research institutions, without undue delay. However, enforcing the right to erasure has proven challenging. Service providers maintain personal data without disclosing the real storage address, making it difficult to verify whether the requested data is indeed deleted. In some cases, service providers may refuse to delete customer data on their servers or in the cloud due to monetary benefits, particularly when the data holds high value. Despite the right to erasure, service providers lack motivation to delete data, leaving customers concerned about the leakage of their uncontrollable personal data. The difficulty of regulation could be one reason why the PIPEDA [2] does not grant Canadians the right to be forgotten. In this report, our aim is to understand the real needs of customers regarding the right to erasure and the implementation of the right to be forgotten. Our contributions are as follows:

- We propose a study on the right of erasure in current privacy laws, including Canada's PIPEDA and CPPA, EU's GDPR, US's ECPA and CCPA, China's PIPL, Japan's APPI, and UK's DPA, comparing the differences in statements about personal information, right to be informed, right of access, right of modification, and right to erasure in these privacy laws.
- We introduce the implementation methods of the right of erasure on 35 platforms, including WhatsApp, LinkedIn, Twitter, Meta, Manulife, Bell, Apple, etc., and summarize the existing methods: account setting, written request, email, inquiry form, contact the IT team, or mixed.
- We design an online survey about the right to be forgotten and proof of erasure, comprising 18 questions to collect knowledge from the general public regarding data deletion policies they seek and their concerns about personal data management policies of government, tech giants, and research institutions.
- We present the survey results, which demonstrate the general public's concerns about privacy leakage, their understanding of privacy policies, their usage of data deletion methods, their need for the right to be forgotten, and their recognition of the importance of proof of erasure.

1. Introduction to Privacy Laws

In this section, we introduce the privacy laws of several countries, including Canada's PIPEDA and CPPA, EU's GDPR, US's ECPA and CCPA, China's PIPL, Japan's APPI, and the UK's DPA.

1.1 GDPR

The GDPR, came into effect on May 25th, 2018, expanded scope of application from the Jus soli of the 1995 "EU Data Protection Directive" to the Jus sanguinis, along with the implementation of a more stringent penalty mechanism, prompted businesses not previously subject to the EU Data Protection Directive to take necessary compliance measures. Many such businesses have now embraced the study of the GDPR to minimize compliance risks due to the expanded territoriality and the imposition of more severe fines. [1]

According to the GDPR, every data processing activity within its purview must adhere to seven data processing principles: (1) fairness, transparency, and legality; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability and compliance. These seven principles, listed in Chapter 2 of the GDPR, form the cornerstone of a company's compliance program and are essential for ensuring privacy protection. Data controllers and processors must rigorously follow these rules, as failure to do so can result in serious infringements punishable by a maximum fine of 20 million euros or 4% of global turnover.

Personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

1.2 PIPEDA

The PIPEDA is the federal privacy law governing private-sector organizations. It establishes the fundamental principles that businesses must adhere to while handling personal information in their commercial activities. [2] PIPEDA regulates how private sector organizations collect, use, and disclose personal information for commercial purposes. Additionally, the Act includes provisions to facilitate the use of electronic documents. PIPEDA came into effect on April 13, 2000, with the aim of promoting consumer trust in electronic commerce.

In PIPEDA, “personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs).”

1.3 CPPA

The CPPA is the new regulations for the gathering, sharing, and utilization of data introduced by the Digital Charter Implementation Act (Bill C-11). It is proposed to enhance oversight of Canadian private sector organizations' business operations and provide stronger protections for the personal information of Canadian citizens [3]. Parts of the PIPEDA would be repealed under this new legislation. The primary purpose of CPPA is to establish clear rules in a time when data

continuously flows across borders and geographical boundaries, and significant economic activity relies on the analysis, circulation, and exchange of personal information. These rules aim to safeguard personal information while respecting individuals' right to privacy and recognizing the legitimate needs of organizations to collect, use, or disclose personal information for purposes that a reasonable person would deem appropriate in the given circumstances. Personal information means “information about an identifiable individual.”

1.4 ECPA

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred to together as the ECPA of 1986. The ECPA was a significant update to the Federal Wiretap Act of 1968, which primarily focused on intercepting conversations using traditional "hard" telephone lines and did not cover the interception of digital and electronic communications. In response to the rapid advancements in communication technologies, subsequent legislation, including The USA PATRIOT Act, has further refined and modernized the ECPA to accommodate new methods and technologies, including granting law enforcement more accessible access to stored communications in certain cases. [4]

Despite these amendments, there is no specific professional regulation within the ECPA that directly addresses the handling of personal information.

1.5 CCPA

The CCPA stands out as the most robust data protection regulation in the U.S., implementing significant changes akin to the EU's GDPR. Both laws are designed to effectively safeguard consumers' personal data and apply to companies that gather, use, or exchange consumer data, whether collected online or offline. However, there are notable differences between the CCPA and GDPR, especially regarding their scope, the types of data collection restrictions, and the regulations governing accountability. [5]

Under the CCPA, companies acting as data service providers are exempt from its provisions if they meet two specific criteria: a) The data controller must inform consumers in the privacy provision that the data service provider will receive their collected personal information. b) The data service provider is prohibited from further collecting, selling, or using the consumer's personal information beyond what is necessary to achieve a business objective.

California residents now enjoy additional rights concerning their personal information. For instance, the CCPA empowers individuals to refuse businesses the right to sell their personal data and provides them with the option to view and delete any personal information collected about them. The CCPA defines the term "sale" broadly, encompassing various instances of data sharing, even when no monetary exchange takes place, making the right to opt-out of such activities essential.

Personal information is “information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints,

and inferences from other personal information that could create a profile about your preferences and characteristics."

Sensitive personal information is "a specific subset of personal information that includes certain government identifiers (such as social security numbers); an account log-in, financial account, debit card, or credit card number with any required security code, password, or credentials allowing access to an account; precise geolocation; contents of mail, email, and text messages; genetic data; biometric information processed to identify a consumer; information concerning a consumer's health, sex life, or sexual orientation; or information about racial or ethnic origin, religious or philosophical beliefs, or union membership. Consumers have the right to also limit a business's use and disclosure of their sensitive personal information."

1.6 PIPL

The China PIPL was formally adopted on August 20th, 2021, and will go into effect on November 1st of the same year. PIPL provides several protections for personal information, with a particular focus on safeguarding the rights and interests of natural persons. Notably, it is the first law in China that specifically regulates the protection of personal information, having a direct impact on the privacy rights of Chinese citizens and data privacy compliance for various organizations. [6]

The officially adopted PIPL establishes comprehensive guidelines for handling personal information, covering aspects such as handling procedures, cross-border data transfers, individual rights, processor obligations, departments responsible for protection, and legal responsibilities. It also places special emphasis on guidelines for handling personal information by state agencies and handling sensitive personal information. By defining these guidelines and requirements for businesses and other personal information processors, as well as outlining the legal responsibilities for violations and infringements, the PIPL takes the crucial first step in safeguarding individuals' rights concerning their personal information.

The PIPL governs various processes related to personal information, including collection, storage, usage, processing, transmission, provision, disclosure, and other activities. Additionally, the law introduces the concept of erasure processing, emphasizing the ethical standards that personal data processors must adhere to. These standards encompass aspects such as lawfulness, legitimacy, necessity, good faith, purpose restriction, minimal necessity, openness and transparency, accuracy, and due diligence.

1.7 APPI

Japan passed one of the earliest personal information protection laws in Asia and globally in 2003, known as the APPI [7]. The primary objective of the APPI is to promote the appropriate and efficient use of personal information while safeguarding the rights and interests of individuals whose data is being utilized. The fines associated with violations of this law were set at up to 500,000 yen before the 2020 amendment, but they have been increased to 100 million yen with the recent revision. Compared to stricter data protection laws such as the GDPR, the APPI imposes fewer requirements on operators and employs less severe penalties.

To further protect personal information and encourage responsible data handling practices, Japan established the Personal Information Protection Committee (PPC) in 2016. This committee plays a crucial role in overseeing and ensuring the effective implementation of the APPI and maintaining a secure and trustworthy environment for personal data usage in the country.

Personal information means "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information including such (information as will allow easy reference to other information and will thereby enable the identification of the specific individual.)"

1.8 DPA

The DPA was officially enacted by the UK on May 23, 2018. This Act serves multiple purposes, including the repeal of the 1998 Data Protection Act, reinstating the UK data protection framework to facilitate the successful implementation of the GDPR within the UK, and allowing for certain customization of GDPR framework rules. [8] Moreover, considering the need for data exchange between the UK and EU nations post-Brexit, it becomes essential to ensure that the UK upholds the same privacy standards as the EU. In this context, the DPA 2018 includes significant updates aimed at strengthening the right of data subjects to have control over their personal data, which stands as a key component of this legislation. Additionally, the Act places greater responsibilities on data controllers to handle personal data responsibly and transparently.

Furthermore, the DPA 2018 establishes a unique enforcement framework concerning the processing of data by criminal justice authorities for legal purposes. This framework underscores the importance of safeguarding personal information even in cases where data processing is carried out by law enforcement agencies.

Overall, the DPA 2018 represents a comprehensive and important step towards enhancing data protection and privacy rights within the UK while ensuring alignment with the GDPR and maintaining compatibility with EU data privacy standards.

"Personal data" means "any information relating to an identified or identifiable living individual."

"Identifiable living individual" means "a living individual who can be identified, directly or indirectly, in particular by reference to (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual."

2 Right to be Forgotten in Privacy Acts

Now we discuss the right to be forgotten in different privacy acts.

2.1 GDPR

In GDPR, the right to erasure is defined as "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay." [1] The following grounds [1] applies:

1. Personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
2. The data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing.
3. The data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2).
4. The personal data has been unlawfully processed.
5. The personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
6. The personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Data controllers have a dual responsibility when it comes to data deletion. Not only are they obligated to delete the data they directly control, but they must also ensure that any data they have publicly disseminated is removed and that third-party recipients are informed to do the same. If the controller has made personal data public and is required to erase it, they must take reasonable steps, considering available technology and implementation costs, to notify other controllers processing the data. This notification should prompt them to erase any links, copies, or replications of the personal data in question.

The GDPR introduces the concept of the "right to be forgotten," which is an expansion of the traditional right to erasure. It encompasses a one-to-many approach, covering both the right to have data deleted by the data controller and the right to request that the controller takes appropriate measures to delete unlawfully collected personal data. This comprehensive approach ensures that individuals have greater control over their personal information and provides them with stronger protections under the GDPR's data protection framework.

2.2 PIPEDA

PIPEDA mentions that private sector organizations and federal institutions can collect personal information about citizens, employees, clients, and prospective clients. Meanwhile, organizations and institutions need to inform the data owners about how to use it, how long to keep it, and when and how to dispose of it. However, PIPEDA does not define the right to be forgotten or similar right that enables data owners to request the data controller to delete their data.

The PIPEDA only states that “personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.” Moreover, Paragraph 4.7.5 specifies that “care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information, which means the organization should dispose personal information securely”. There are common methods for organizations to properly dispose of personal information, including disintegration, incineration, pulverizing, shredding, melting, overwriting, and degaussing. In short, the PIPEDA states that the data controller has the responsibility to delete the data and handle the dispose of personal information.

2.3 CPPA

CPPA states that “an organization must not retain personal information for a period longer than necessary to

a) fulfill the purposes for which the information was collected, used, or disclosed; or
b) comply with the requirements of this Act, of federal or provincial law or of the reasonable terms of a contract. The organization must dispose of the information as soon as feasible after that period.”

It is noticeable that the CPPA defines the similar principle of the right to be forgotten. That is, “if an organization receives a written request from an individual to dispose of their personal information that is under the organization’s control, the organization must, as soon as feasible, dispose of the information, if

(a) the information was collected, used or disclosed in contravention of this Act;
(b) the individual has withdrawn their consent, in whole or in part, to the collection, use or disclosure of the information; or
(c) the information is no longer necessary for the continued provision of a product or service requested by the individual.”

Moreover, if an organization fulfills the individual's request to dispose of their personal information, it must also take prompt action to notify any service provider to which it had previously transferred the information. The organization must ensure that the service provider promptly disposes of the information as well.

2.4 ECPA

In ECPA, there is no definition about personal data or specific professional regulation that directly addresses the handling of personal information. Also, there is no definition of the right to be forgotten.

2.5 CCPA

The "Consumers' Right to Delete Personal Information" refers to the right of consumers in California to request the deletion of their personal data. Offshore companies operating in California must have a dedicated team to promptly respond to such inquiries and maintain accurate records of the requests.

Furthermore, businesses are required to inform their customers explicitly about their right to be forgotten. When a company receives a request from a customer to delete personal information, it should verify the request's authenticity and proceed with deleting the data. Simultaneously, the company should request that other data service providers also delete the relevant information. It's important to note that a business is not obligated to erase personal information if it is necessary to retain it to complete a transaction or provide goods or services. This exception is significant and allows businesses to retain relevant information required for legitimate purposes. The detailed principles of the right to be forgotten are defined as follows:

“a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”

“b) A business that collects personal information about consumers shall disclose the consumer’s right to request the deletion of the consumer’s personal information.”

“c) 1. A business that receives a verifiable consumer request from a consumer to delete the consumer’s personal information pursuant to subdivision a) of this section shall delete the consumer’s personal information from its records, notify any service providers or contractors to delete the consumer’s personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer’s personal information unless this proves impossible or involves disproportionate effort.”

“2. The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.”

“3. A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete and shall notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors, or third parties who may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer’s personal information unless this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer’s personal information in its role as a service provider or contractor to the business.”

2.6 PIPL

The PIPL clearly states the agreement between the individuals and the personal information handlers about data collection, storage, and usage. Article 21 of PIPL states “where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted person on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted person. Without the consent of the personal information handler, an entrusted person may not further entrust personal information handling to other persons.”

PIPL defines the right to be forgotten that enables individuals to request the deletion if the personal information handlers do not proactively delete them. Article 47 of PIPL states “personal information handlers shall proactively delete personal information where one of the following circumstances occurs; if the personal information handler has not deleted it, individuals have the right to request deletion:

a) The handling purpose has been achieved, is impossible to achieve, or [the personal information] is no longer necessary to achieve the handling purpose.

b) Personal information handlers cease the provision of products or services, or the retention period has expired.
c) The individual rescinds consent.
d) Personal information handlers handled personal information in violation of laws, administrative regulations, or agreements.
e) Other circumstances provided by laws or administrative regulations."

2.7 APPI

The APPI defines should keep personal data accurate and delete it if it is not needed. Specifically, Article 19 states "a personal information handling business operator shall strive to keep personal data accurate and up to date within the scope necessary to achieve a utilization purpose, and to delete the personal data without delay when such utilization has become unnecessary." Meanwhile, Article 35-2 (5) mentions that "a pseudonymously processed information handling business operator shall strive to delete personal data that are pseudonymously processed information and deleted information etc. without delay when utilization of the personal data and the deleted information etc. has become unnecessary."

In addition, individuals can request the business operator to make a correction, addition or deletion if the contents of retained personal data are not factual.

APPI has defined several citizens' rights regarding their personal data [7], including:

a) "The right to request an organization cease the use or transfer of their personal data if the organization no longer has a valid reason to use the data, a data breach has occurred, or the handling of said data will infringe upon the data subject's rights.
b) The right to access personal data an organization wishes to delete within six months.
c) The right to request access to records pertaining to data transfers to third parties.
d) The right to request a copy of any personal information relating to the data subject."

2.8 DPA

The right to erasure or restriction of processing mentioned in DPA includes:

1) "The controller must erase personal data without undue delay if the processing of the personal data would infringe section 35, 36(1) to (3), 37, 38(1), 39(1), 40, 41 or 42, or the controller has a legal obligation to erase the data.
2) Where the controller would be required to erase personal data under subsection (1) but the personal data must be maintained for the purposes of evidence, the controller must (instead of erasing the personal data) restrict its processing.
3) Where a data subject contests the accuracy of personal data, but it is not possible to ascertain whether it is accurate or not, the controller must restrict its processing.
4) A data subject may request the controller to erase personal data or to restrict its processing (but the duties of the controller under this section apply whether or not such a request is made)."

2.8 Comparisons

Privacy Laws	GPDR	PIPEDA	CPPA	ECPA	CCPA	PIPL	APPI	DPA
Personal Data Definition	✓	✓	✓	×	✓	×	✓	✓
Proactive Data Deletion	✓	✓	✓	×	✓	✓	✓	✓
Right to be Forgotten	✓	×	✓	×	✓	✓	×	×
Verifiable Data Deletion	×	×	×	×	×	×	×	×

3 Deployment of the Right to be Forgotten

3.1 Deployment Methods

We collected the privacy policy statements and the deployed methods of the right to be forgotten on 35 platforms, grouped based on their services. The methods identified are as follows:

- Account Setting: The user can delete the account on systems or apps.
- Email: The user needs to send emails to the companies or organizations to request the deletion of personal information.
- Written request: The user needs to write a request and mail it to the companies or organizations to request the deletion of personal information.
- Inquiry form: The user needs to fill in an inquiry form and submit it to the companies or organizations to request the deletion of personal information.
- Contact us: The user needs to call customer support of the companies or organizations to request the deletion of personal information.

The conditions for data deletion include:

- The number of days that the personal information will be kept on the servers after the request has been received.
- The laws and guidelines for companies or institutions on the management of personal information.
- The needs of the companies or organizations regarding personal information for managing products and services.

3.2 Deployment of Services

We conducted a sample study comprising 35 companies, categorized into 10 social platforms, 10 financial, 10 technical, and 4 government organizations. Based on this sample, we observed five distinct types of current implementation methods for data deletion: 1) deleting data via account setting, 2) using email communication, 3) submitting a written request, 4) filling out an inquiry

form, and 5) contacting customer support. The summary of these methods is presented in the following table.

Social Media	Deployed Methods	Types	Condition Apply
Twitter	account setting	user control	N
WhatsApp	account setting	user control	N
Pinterest	Contact us	by request	Y
LinkedIn	Contact us	by request	N
Tumblr	account setting	by request	Y
Flickr	Contact us	by request	N
Meta	account setting	user control	N
Discord	account setting	user control	Y
TikTok	account setting	user control	N
Reddit	email	by request	N
Snapchat	account setting	user control	N

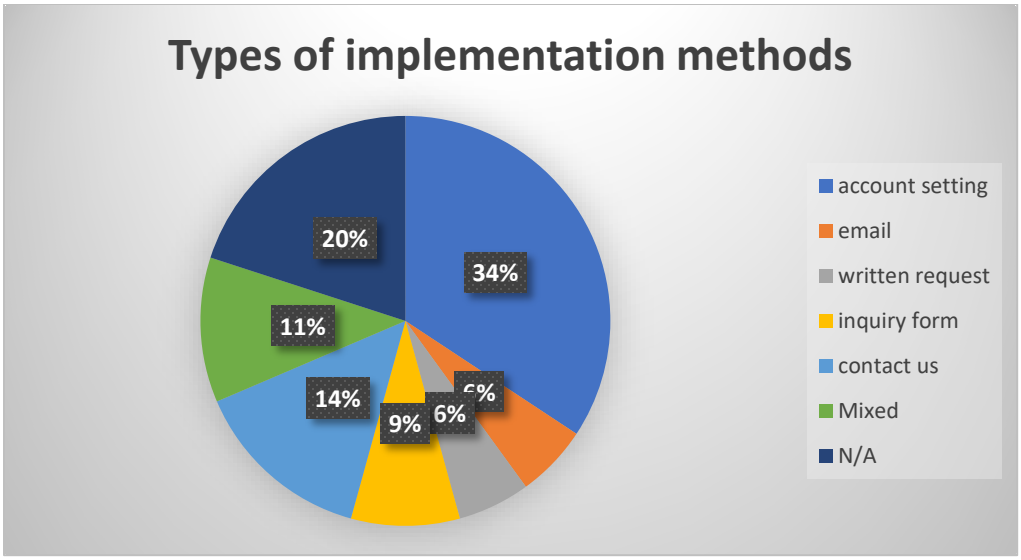
Finance	Deployed Methods	Types	Condition Apply
Bloomberg	Inquiry form	by request	Y
Manulife	written request	by request	Y
TD Bank	written request	by request	Y
Sunlife	Contact us	by request	N
FaithLife	N/A	N/A	N/A
JD Morgan	N/A	N/A	N/A
Well's Fargo	Contact us + inquiry form	by request	N/A
Capital One	account+inquiry	by request	N
Discovery Financial Inc.	Contact us + inquiry form	by request	N
PNC Financial	Contact us	by request	N

Technical	Deployed Methods	Types	Condition Apply
Clio	email	by request	Y
Bell	N/A	N/A	N/A
Apple	account setting	user control	Y
Google	account setting	user control	N
NVIDA	account setting	user control	N

Microsoft	account + contact	user control+by request	N
Yandex	account setting	user control	Y
Tesla	account setting	user control	N
Cisco	inquiry form	by request	N
Adobe	inquiry form	by request	Y

Government	**Deployed Methods**	**Types**	**Condition Apply**
Canada Post	N/A	N/A	Y
Government of Canada	N/A	N/A	Y
Government of Ontario	N/A	N/A	Y
Canadian Transportation Agency	N/A	N/A	Y

Current Implementation Methods	**# of companies applied**
account setting	12
email	2
written request	2
inquiry form	3
contact us	5
Mix of them	4
N/A	7
	total=35



From the table above, it is evident that the "Account Setting" method is the most widely used approach for users to exercise their data deletion right (right to be forgotten), and this method is adopted by most social media companies. However, all governmental organizations do not make any statement or provide a way for users to request the deletion of their data.

Regarding the rights to erasure in Discord, besides offering a way to delete data by deleting the account, it also provides an automated scheme wherein users' data would be deleted if their accounts remain inactive for more than two years. This data deletion scheme is commendable as it fulfills the right of erasure without requiring users to submit deletion requests themselves. In other words, for those concerned about their data privacy, they need not worry about whether their data will be deleted, even if they have not actively requested it.

On the other hand, it is observed that all governmental agencies do not provide a way for users to request data deletion. The reason behind this is that most of the data processed by the government is done as a result of legal obligations or to carry out public tasks, and users cannot request the deletion of this data.

4 Online Survey

Data Security and Privacy Survey: Knowledge on the Right to be Forgotten.

Nowadays, technology companies (e.g., Google, Facebook, and Apple) and institutions (e.g., banks, immigration offices, and government) collect a large amount of data from your devices, such as mobile phones, smart watches, and personal computers. For example, Google stores your personal emails on Gmail, your browsing history on Chrome, and your watch history on YouTube. However, you may never know how they use the collected data and whether they delete it after usage. You are being invited to participate in a research study about the understanding of the general public about the right of data deletion on the Internet (i.e., you have the right to require the companies or institutions to delete your data in the accounts or the collected data about your online activities), the deployment methods of the right to erasure your data on the existing data platforms (e.g., account deletion, ask the platforms via emails or written forms), and the expected policies of personal online data deletion that the general public is seeking for. This study is being conducted by Dr. Jianbing Ni, from the Department of Electrical and

Computer Engineering at Queen's University, Canada. The study is being conducted as part of a research project funded by the Office of the Privacy Commissioner of Canada.
There are no known risks if you decide to participate in this research study. There are no costs to you for participating in the study. The information you provide will be used for the study of the right to be forgotten and the expectation of the general public for personal data deletion. The questionnaire will take approximately 10 minutes to complete. The information collected may not benefit you directly, but the information learned in this study should provide more general benefits.

This survey is anonymous. Do not write your name on the survey. We will not collect any personal identifiable information except nationality, gender, age, and occupation. IP addresses will not be collected. No one will be able to identify you or your answers, and no one will know whether or not you participated in the study. Should the data be published, no individual information will be disclosed.

Your participation in this study is voluntary. You are free to decline to answer any particular question you do not wish to answer for any reason.

If you have any questions about the study, please contact Dr. Ni (jianbing.ni@queensu.ca).

1. Gender
- Male
- Female
- I do not identify within the gender binary
- I prefer not to disclose information concerning my gender

2. Age
- Below 18
- 18-29
- 30-49
- 50-64
- Above 65
- Decline to answer.

3. Occupation
- Worker
- Teacher
- Professor
- Technician
- Engineer
- Student
- Government staff
- Scientist
- Social Worker
- Lawyer
- Self-employer
- Doctor
- Nurse
- Police officer
- Consultant
- Designer
- Bank staff
- Other

4. What do you think is your personal information? (you can choose multiple answers)

- age, name, ID numbers, home address, phone number, social security number, email address.
- Income, salary
- marital status
- ethnic origin
- political opinions
- online comments
- social status
- disciplinary actions
- education, medical, criminal or employment history
- financial transactions
- records of products purchased
- internet browsing history
- Fingerprints
- location data
- trade union membership
- Decline to answer.

5. Do you worry about the leakage or breach of your account information (e.g., Google, Facebook, Twitter) or your Internet activities (e.g. cookies, watch history, search history, browsing history)? (Strongly worry, a little worry, never worry, have no idea, decline to answer)

6. Do you suspect that your personal information (i.e., your data in your account) will be used, copied, shared, saved, or deleted by the platforms, such as Google, Facebook, without informing you or without your permission on usage, copy, sharing, saving, or deletion? (Yes No, have no idea, decline to answer)

7. Did you read the privacy policy (agreement) if you are asked to accept it when installing a mobile APP or accessing Internet services (e.g., GMail, Facebook, and iCloud)? (Carefully read, briefly read, read sometime, never read, do not know what it is, decline to answer)

8. Do you know the right to be forgotten in General Data Protection Regulation (GDPR) of Europe Union, California Consumer Privacy Act (CCPA), or Personal Information Protection Law (PIPL) of the People's Republic of China. (Yes, No, decline to answer)
The right to be forgotten: You shall have the right to obtain from a technical company or institution the erasure of personal data you concern without undue delay and the company shall have the obligation to erase personal data without undue delay.

9. The right to be forgotten defines your right that you can ask a company/institution to erase the personal data that you concern with without undue delay, or a company/institution has the obligation to erase personal data without undue delay. Do you think the right to be forgotten is needed? (Yes, No, have no idea, decline to answer)

10. Do you think when you shall have the right to request deletion of your data collected by some companies, institutions, or organizations? (You can choose multiple answers)
- The personal data are no longer needed for those parties, or the purpose of processing has been achieved;
- You withdraw consent on data collection to those parties;
- You delete your data (e.g., documents or photos) on the cloud or the storage period you purchased from the cloud storage services (e.g., Dropbox, One Drive) has expired.
- The companies or organizations do not follow the purposes agreed with you to use, share, or process your personal data.

- The usage or processing of personal data becomes unlawful based on some laws, the personal information processor (e.g. GMail, Facebook, and iCloud) processes personal information in violation of laws, administrative regulations, or the agreement.
- The personal data have been collected in relation to the offer of information society services (e.g., online storage, social networks, hotel or flight booking services, online search, online news, advertising, e-mails other than personal e-mails).
- decline to answer

11. Do you ever or will use the right to be forgotten, i.e., ask the company, such as cloud storage server or system manager to permanently delete the account or personal data, or delete the account through a series of operations in account setting? (Yes No, decline to answer)

12. Are you aware of where and how to exercise your right to be forgotten, i.e., how to ask the websites or companies deleting your personal information or how to proactively delete the account on social media via a series of operations in account setting? (Yes, No, decline to answer)

13. If you are exercising your right to be forgotten, what kind of methods of data deletion would you prefer? (Delete your account on social networks via a series of operation in account setting, send an email to the website manager to delete your data or account, send a written request to the website manager to delete your data or account, fill and submit an online inquiry form and send to the website manager to delete your data or account, direct contact with calls to the website manager to delete your data or account, others, decline to answer)

14. Do you think "the right to be forgotten" will help you to protect your personal information? (Yes, do not care, No, decline to answer)

15. Do you worry that the company still keeps your personal data even if you have deleted the account in account setting or asked them to delete your personal data via email or call? (Strongly worry, a little worry, not worry, have no idea, decline to answer)

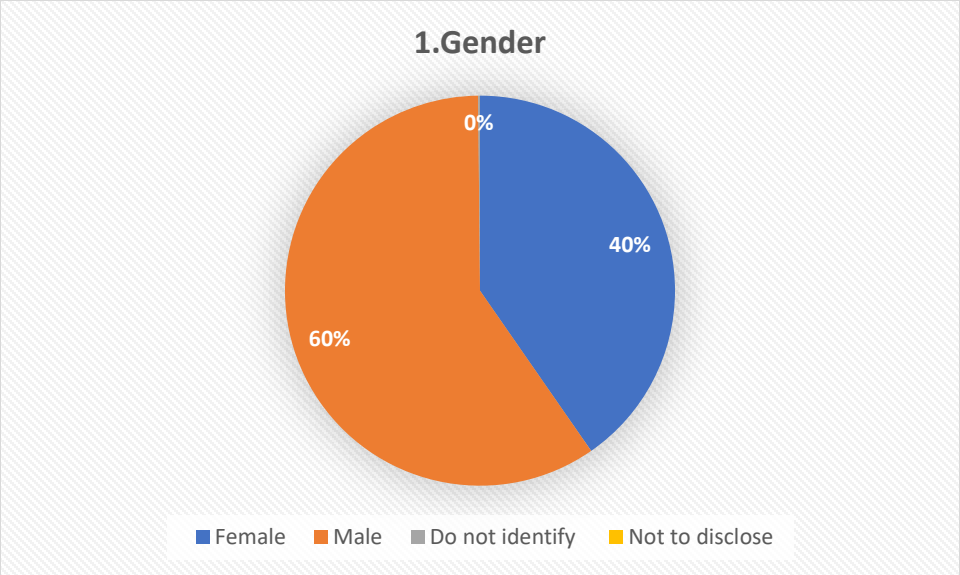
16. Did you still receive any promoted advertisement or product recommendation on your social media (e.g. email, phone text, website page) after you delete your account/personal data or you close the "user preference" option? (Yes, No, have no idea, decline to answer)

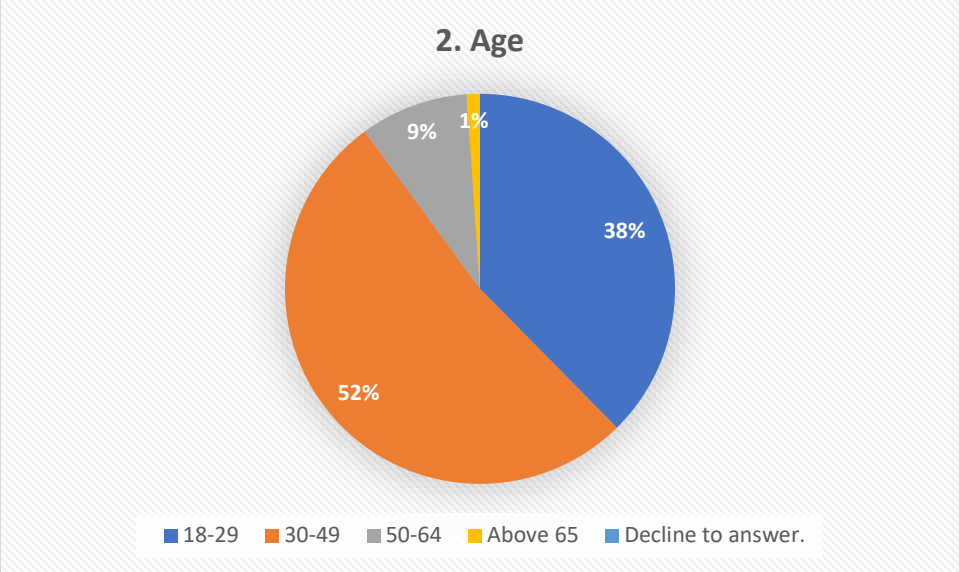
17. Do you think "the proof of erasure" is needed? (Yes No, have no idea, decline to answer)
The proof of erasure: You should have the capability to verify whether accounts or personal information are really deleted by the company or institution after you delete the online account in account setting or requests the company to delete them.

18. If you are provided with the capability that can verify if accounts or personal information are deleted after data deletion operation, will you use it? (Yes, No, have no idea, decline to answer)

5 Survey Results

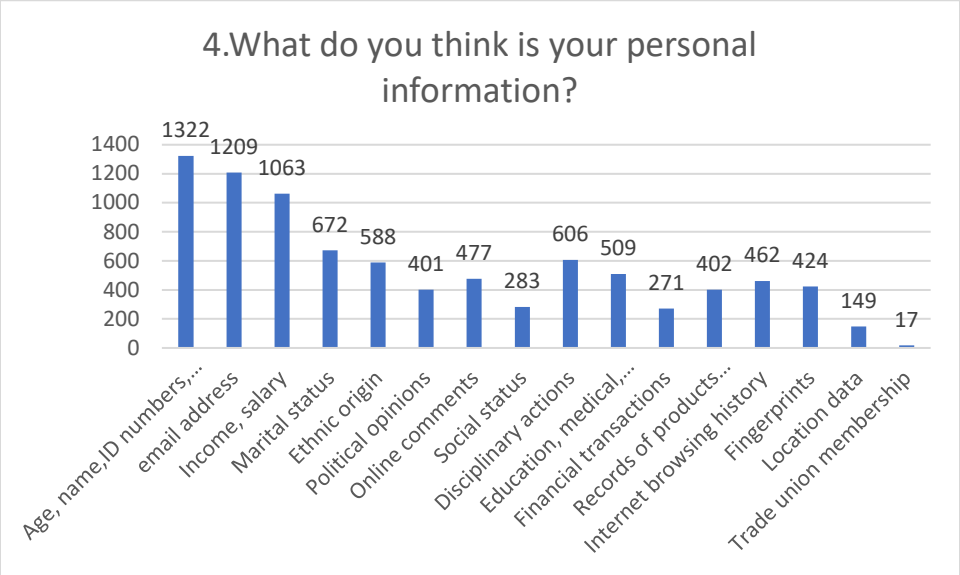
We conducted an online survey on the Amazon MTurk platform and received 2197 responses from platform users worldwide. We thoroughly analyzed each question's answers and have presented the response figures below.

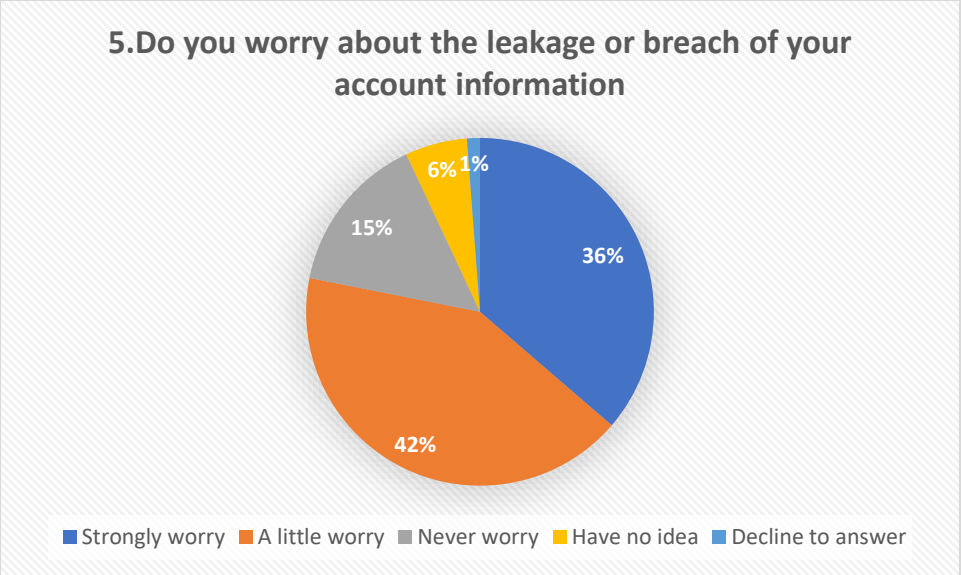


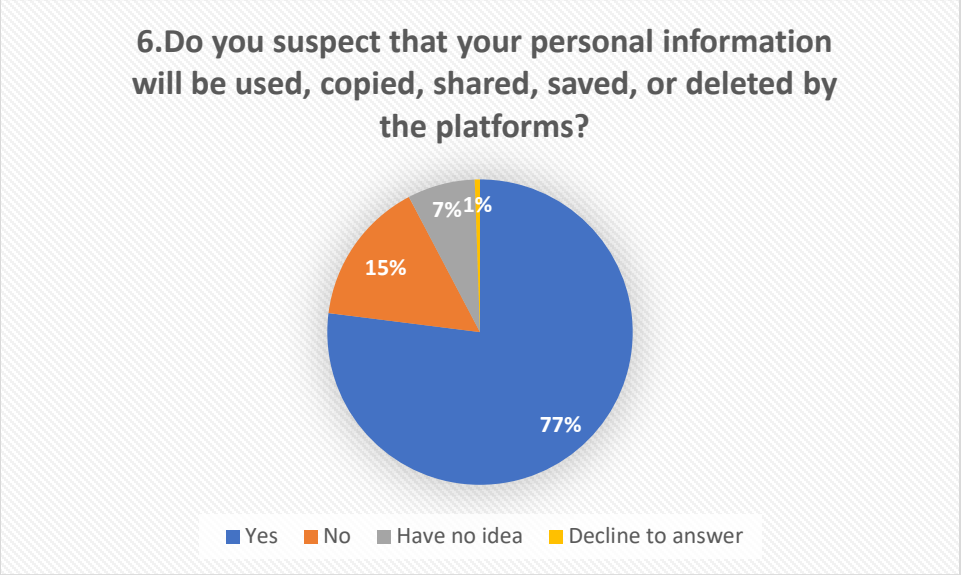


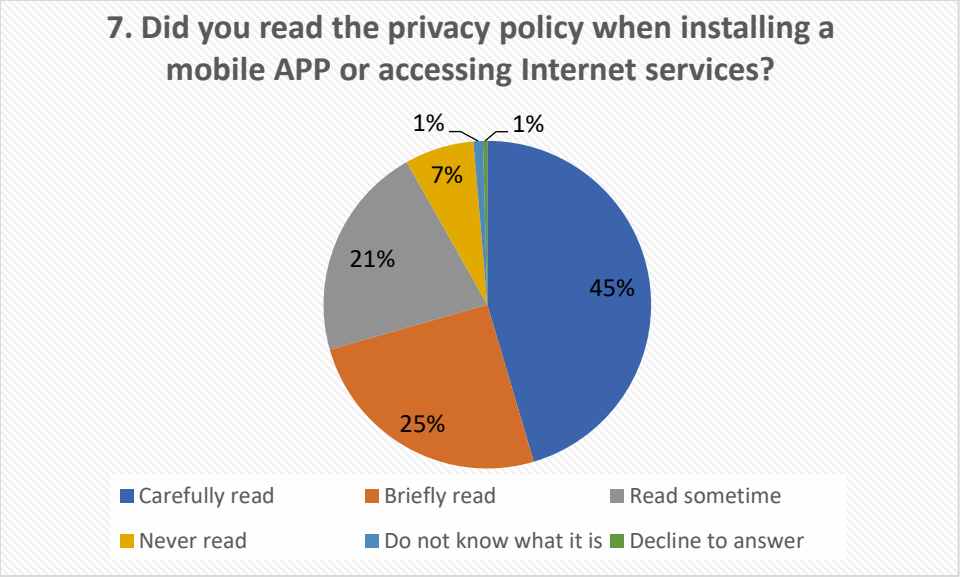
3.Occupation	Number	Column1
Computer and Mathematical Occupations	331	16.56%
Business and Financial Operations Occupations	206	10.31%
Office and Administrative Support Occupations	197	9.85%
Personal Care and Service Occupations	145	7.25%
Education, Training, and Library Occupations	120	6.00%
Management Occupations	116	5.80%
Healthcare Support Occupations	116	5.80%
Healthcare Practitioners and Technical Occupations	114	5.70%
Sales and Related Occupations	81	4.05%
Community and Social Service Occupations	77	3.85%
Construction and Extraction Occupations	68	3.40%
Food Preparation and Serving Related Occupations	66	3.30%

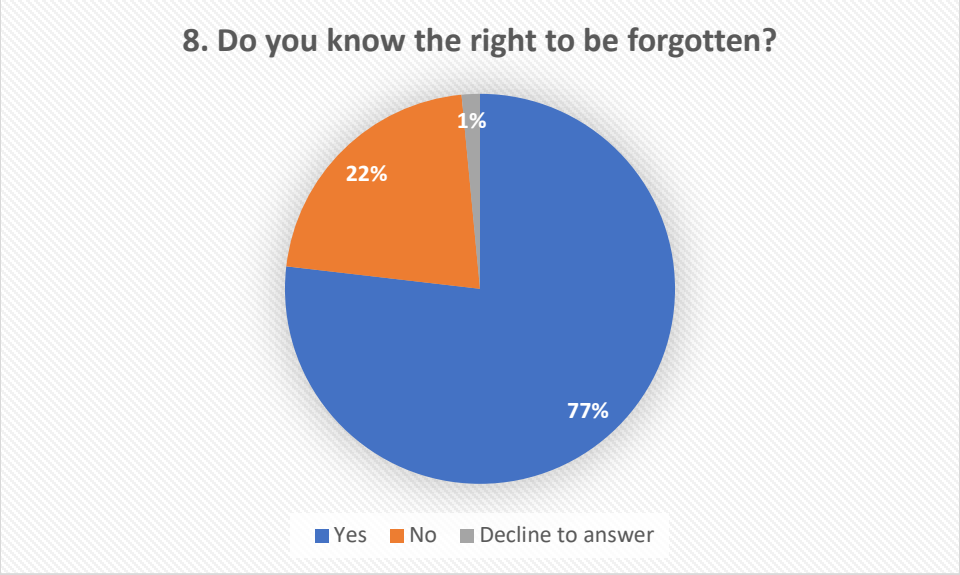
Other	62	3.10%
Installation, Maintenance, and Repair Occupations	60	3.00%
Architecture and Engineering Occupations	52	2.60%
Arts, Design, Entertainment, Sports, and Media Occupations	38	1.90%
Production Occupations	35	1.75%
Protective Service Occupations	30	1.50%
Farming, Fishing, and Forestry Occupations	26	1.30%
Legal Occupations	24	1.20%
Building and Grounds Cleaning and Maintenance Occupations	22	1.10%
Life, Physical, and Social Science Occupations	9	0.45%
Transportation and Materials Moving Occupations	3	0.15%
Comercial financeiras	1	0.05%

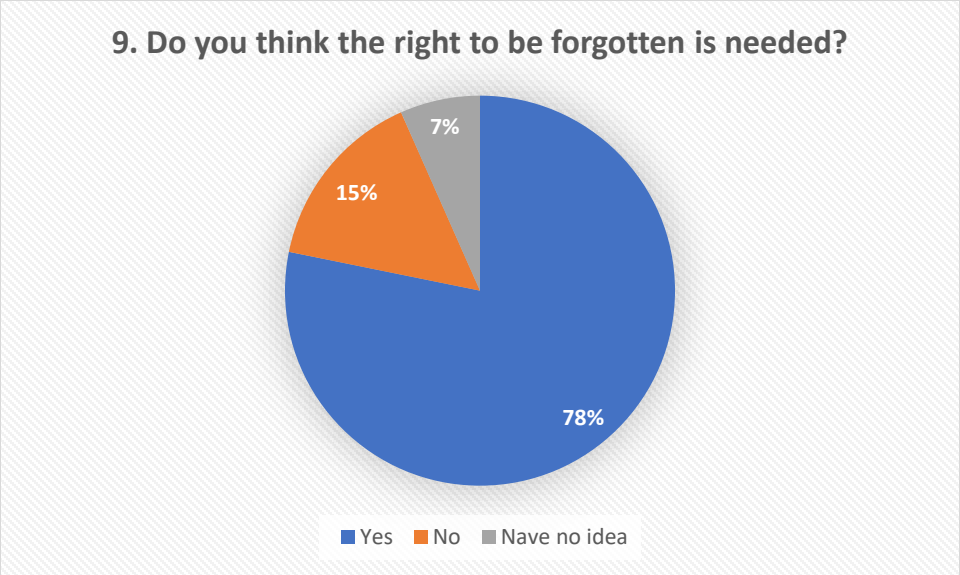


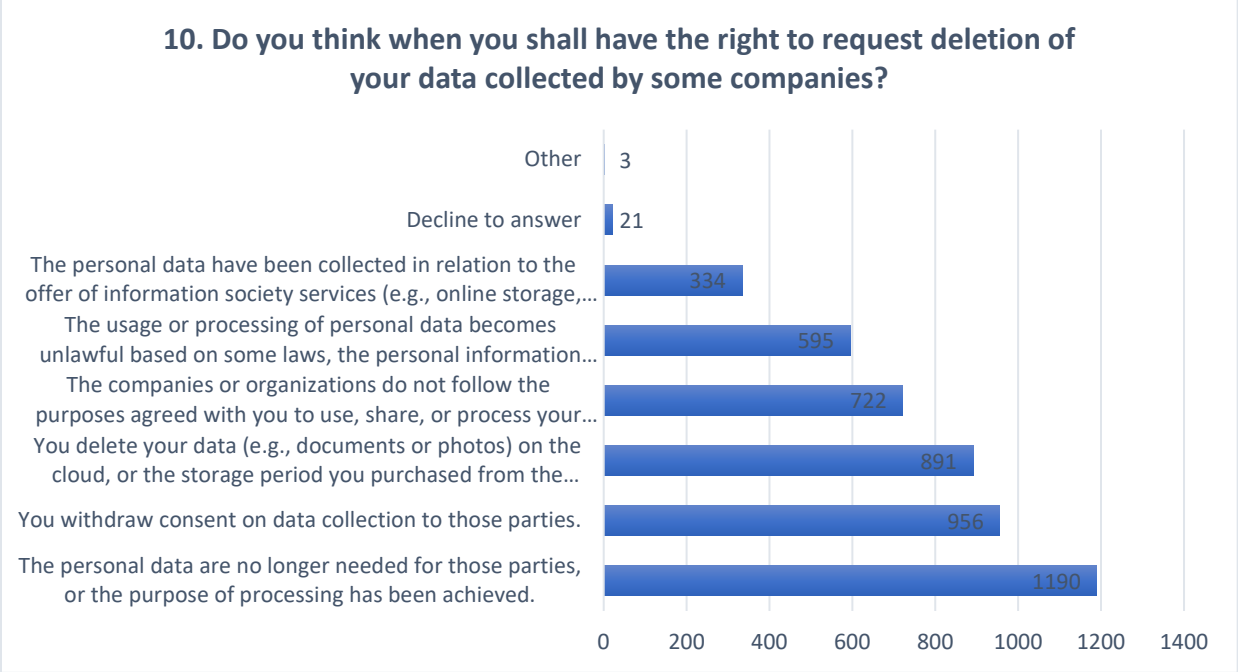

5.Do you worry about the leakage or breach of your account information
36%
42%
15%
6%
1%
Strongly worry
A little worry
Never worry
Have no idea
Decline to answer

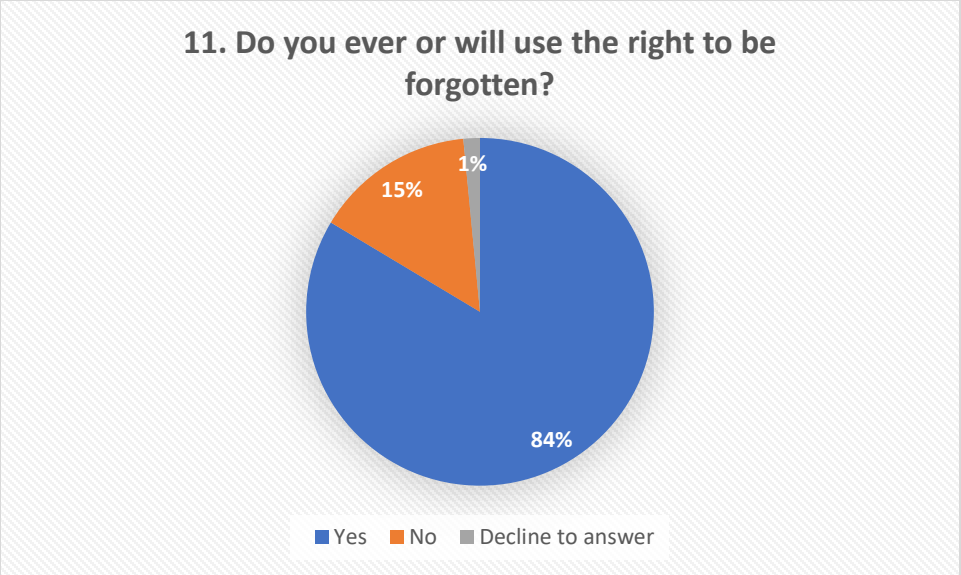

6.Do you suspect that your personal information will be used, copied, shared, saved, or deleted by the platforms?
77%
15%
7%
1%
Yes
No
Have no idea
Decline to answer

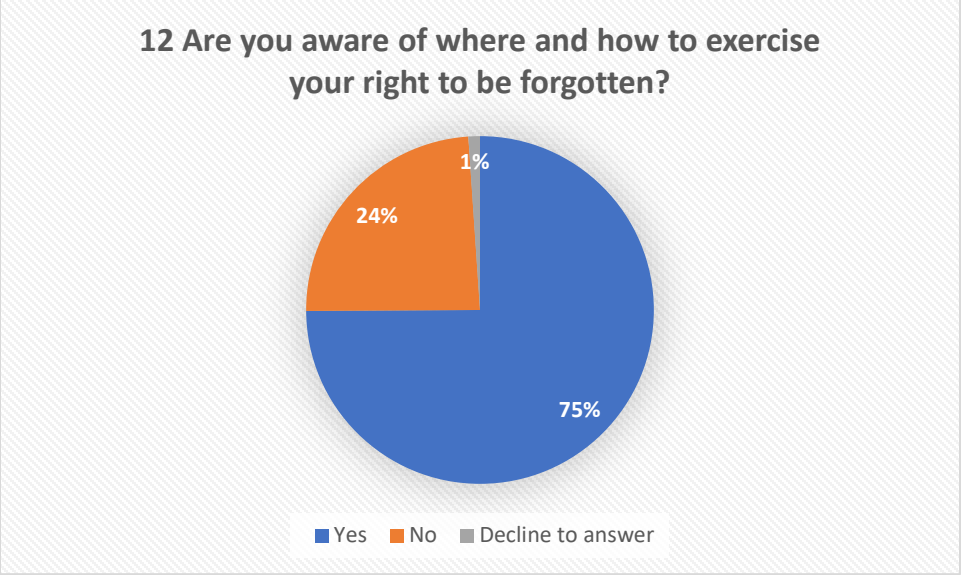

7. Did you read the privacy policy when installing a mobile APP or accessing Internet services?
1%
1%
7%
21%
45%
25%
Carefully read
Briefly read
Read sometime
Never read
Do not know what it is
Decline to answer

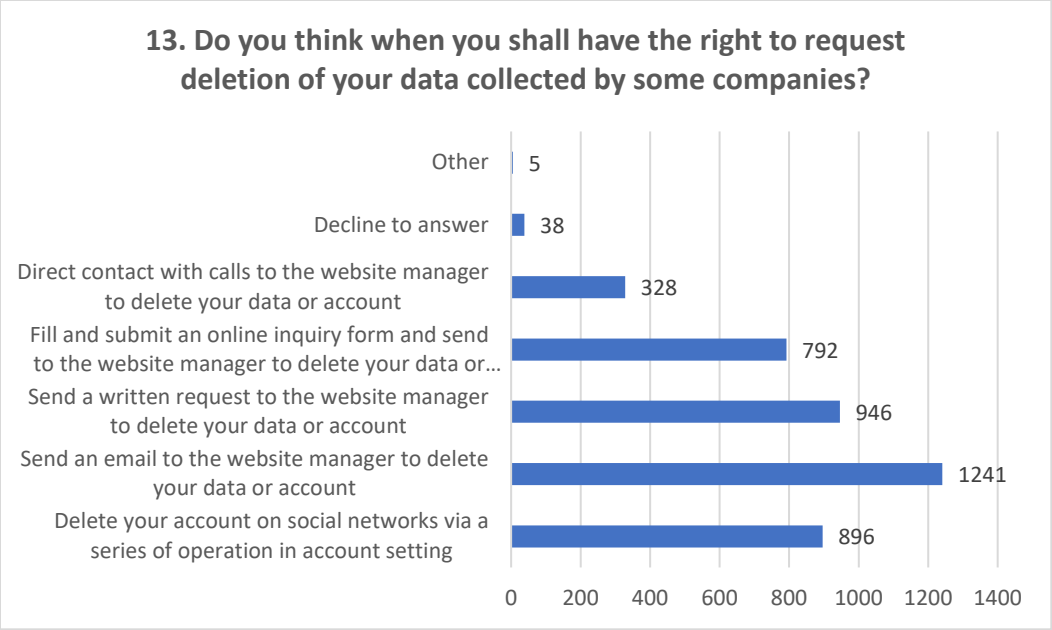

8. Do you know the right to be forgotten?
1%
22%
77%
Yes
No
Decline to answer

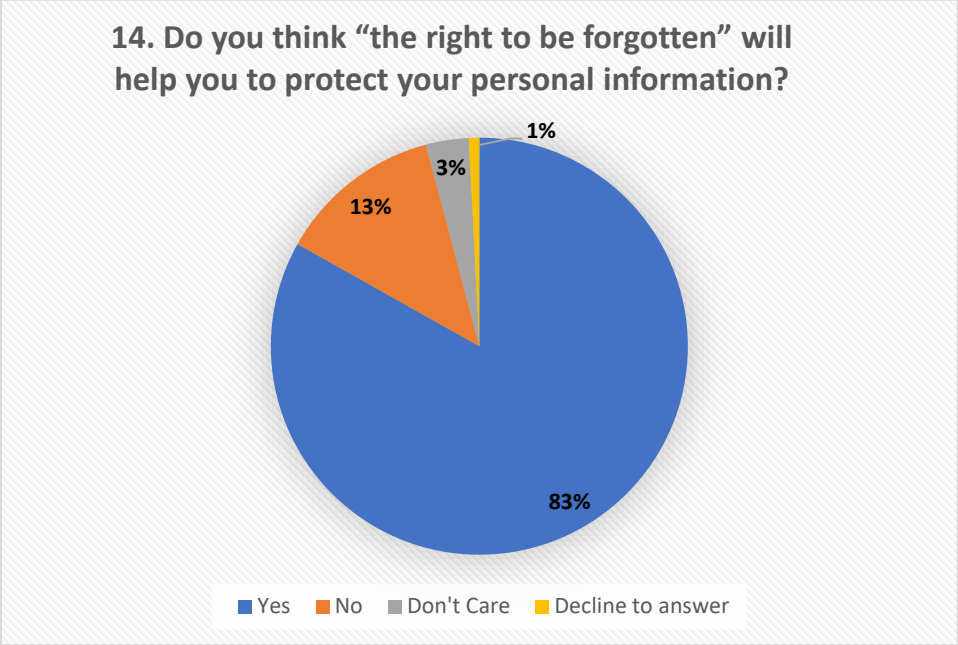

9. Do you think the right to be forgotten is needed?
7%
15%
78%
Yes
No
Nave no idea

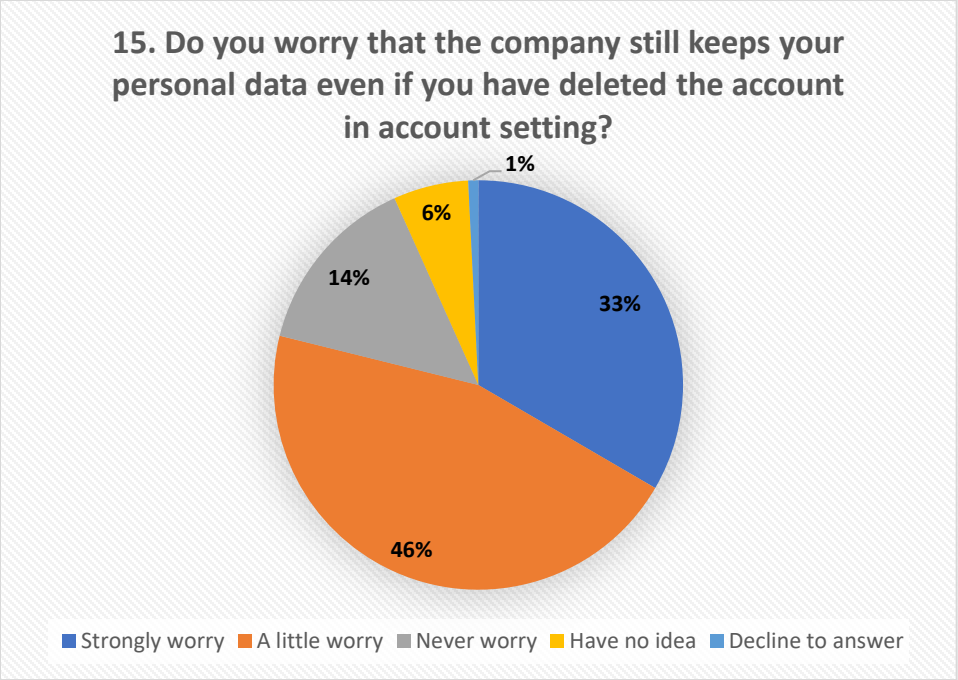

10. Do you think when you shall have the right to request deletion of your data collected by some companies?
Other
3
Decline to answer
21
The personal data have been collected in relation to the offer of information society services (e.g., online storage,...
334
The usage or processing of personal data becomes unlawful based on some laws, the personal information...
595
The companies or organizations do not follow the purposes agreed with you to use, share, or process your...
722
You delete your data (e.g., documents or photos) on the cloud, or the storage period you purchased from the...
891
You withdraw consent on data collection to those parties.
956
The personal data are no longer needed for those parties, or the purpose of processing has been achieved.
1190
0
200
400
600
800
1000
1200
1400

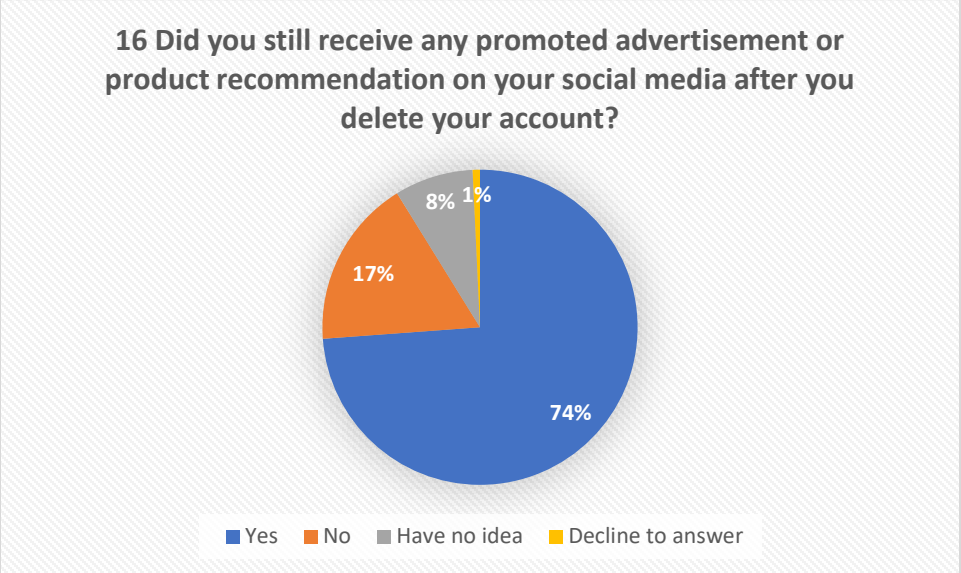

11. Do you ever or will use the right to be forgotten?
1%
15%
84%
Yes
No
Decline to answer

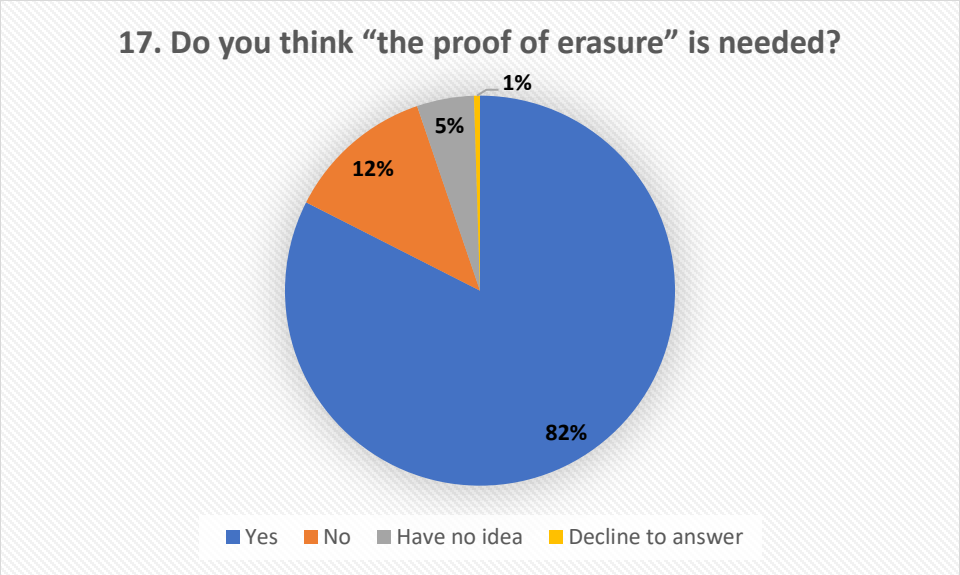

12 Are you aware of where and how to exercise your right to be forgotten?
1%
24%
75%
Yes
No
Decline to answer

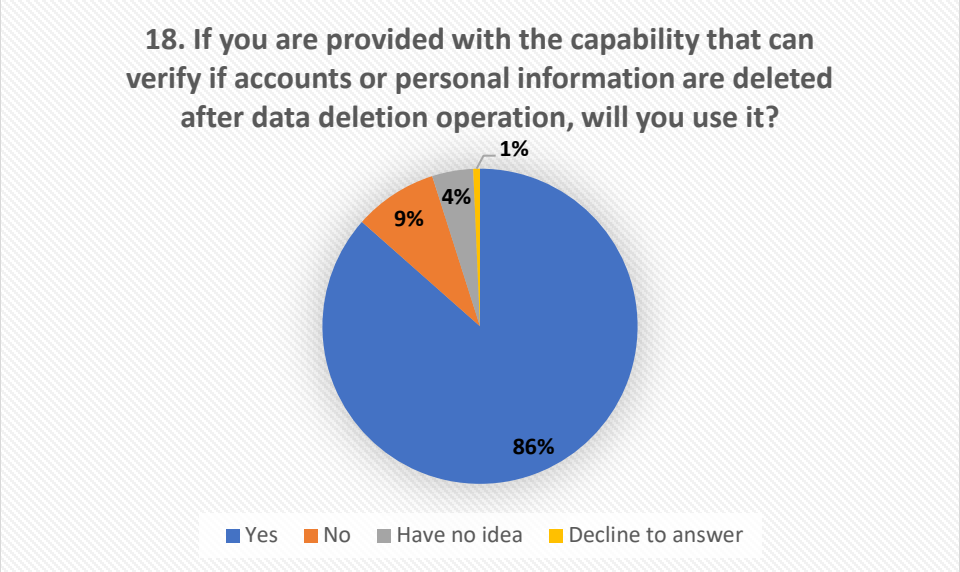

13. Do you think when you shall have the right to request deletion of your data collected by some companies?
Other
5
Decline to answer
38
Direct contact with calls to the website manager to delete your data or account
328
Fill and submit an online inquiry form and send to the website manager to delete your data or...
792
Send a written request to the website manager to delete your data or account
946
Send an email to the website manager to delete your data or account
1241
Delete your account on social networks via a series of operation in account setting
896
0
200
400
600
800
1000
1200
1400


14. Do you think “the right to be forgotten” will help you to protect your personal information?
1%
3%
13%
83%
Yes
No
Don't Care
Decline to answer


15. Do you worry that the company still keeps your personal data even if you have deleted the account in account setting?
1%
6%
14%
33%
46%
Strongly worry
A little worry
Never worry
Have no idea
Decline to answer


16 Did you still receive any promoted advertisement or product recommendation on your social media after you delete your account?
8%
1%
17%
74%
Yes
No
Have no idea
Decline to answer





6 Conclusion

This report presents the results of our study on the right to be forgotten in current privacy laws and its implementation. It includes a detailed comparison of different privacy laws regarding statements on personal information, the right to be informed, the right of access, the right of modification, and the right to erasure. We have also compiled information on the current methods used for the right of erasure on 35 platforms, revealing that most technology companies have deployed this right, while government departments have not.

Additionally, we designed an online survey about the right to be forgotten and proof of erasure, consisting of 18 questions to gather knowledge from the general public. The survey also explores the data deletion policies the public is seeking. We have carefully analyzed the survey results and present our findings in this report.

References

[1] "General Data Protection Regulation," 25 May 2018. [Online]. Available: https://gdpr-info.eu/.
[2] "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96," [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html.
[3] "Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts," [Online]. Available: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading#:~:text=Part%201%20enacts%20the%20Consumer,the%20course%20of%20commercial%20activities..
[4] "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523," [Online]. Available: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=General%20Provisions,conversations%2C%20and%20data%20stored%20electronically..
[5] "California Consumer Privacy Act (CCPA)," [Online]. Available: https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20requires%20business%20privacy,the%20Right%20to%20Non%2DDiscrimination..
[6] "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021," [Online]. Available: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.
[7] "個人情報の保護に関する法律（平成十五年法律第五十七号）," 三十日 五月 平成十五年. [Online]. Available: https://elaws.e-gov.go.jp/document?lawid=415AC0000000057.
[8] "Data Protection Act 2018," [Online]. Available: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[9] "Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts," [Online]. Available: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading#:~:text=Part%201%20enacts%20the%20Consumer,the%20course%20of%20commercial%20activities..