User Account Deletion Mechanisms in the Mobile Internet Environment: Postprint

Authors: Wu Renli, Wu Shuqian

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] In the mobile Internet environment, mobile application (APP) service providers have access to increasingly large amounts of user data. Account cancellation has become an effective means for users to prevent their personal information from being illegally exploited, and the construction of an account cancellation mechanism is of great significance for ensuring user information security. [Method/Process] Based on a systematic investigation of relevant Chinese laws and regulations and the EU GDPR, this study comprehensively reviews the account cancellation mechanisms of mainstream APPs both domestically and internationally, analyzes existing problems, and proposes feasible construction strategies. [Results/Conclusion] This paper proposes a full-process account cancellation mechanism covering three stages: pre-cancellation, during cancellation, and post-cancellation, with collaborative participation from three parties: service providers, regulatory agencies, and users. It also identifies future directions for breakthroughs and innovation in user information security-oriented management and services.

Full Text

Abstract

[Purpose/Significance] In the mobile Internet environment, mobile application (APP) service providers have mastered an increasing amount of user data. Account cancellation has become an effective means for users to prevent illegal utilization of personal information, making the construction of account cancellation mechanisms crucial for safeguarding user information security. [Method/Process] Based on systematic investigations of relevant Chinese laws and regulations and the EU' s GDPR, this study comprehensively reviews account cancellation mechanisms in mainstream domestic and international APPs, analyzes existing problems, and proposes feasible construction strategies. [Result/Conclusion] We propose a full-process account cancellation

mechanism covering three stages—pre-cancellation, during cancellation, and post-cancellation—with collaborative participation from service providers, regulatory agencies, and users. The study also identifies future directions for breakthroughs and innovations in user information security management and services.

Keywords: right to be forgotten; personal data; information protection; data deletion; privacy impact assessment

Introduction

In the mobile Internet era, the proliferation of smart terminals has enabled various APPs to penetrate every aspect of public life. The explosive growth of user privacy data has also made it possible to accurately profile and identify user entities in the information world [1]. Today, social APPs' real-name authentication systems map users' real social networks into virtual space; financial APPs capture users' identity and economic information through ID and bank card binding; and sharing economy APPs allow users to disclose more data and privacy in exchange for convenient services [2]. The data obtained by APP service providers is no longer limited to information actively provided by users, but also includes information generated during usage such as travel routes, browsing history, and personal preferences.

Account cancellation serves as an effective approach to address information abuse, avoid data risks, and strengthen security management in the big data and Internet environment, attracting widespread international attention. Foreign countries not only have dedicated websites evaluating the difficulty of deleting APP accounts [8], but relevant studies [9-11] also consider allowing users to delete accounts as an important measure for controlling personal data, especially when services are no longer used [12] or in cases of "digital death" [13]. Furthermore, the EU' s General Data Protection Regulation (GDPR), which officially took effect in May 2018 [14], establishes legal foundations for account cancellation through data subject rights such as the "right to erasure" and "right to data portability," providing important guidance [15].

In China, policies and practices related to user account cancellation remain imperfect. The public outcry over Baidu CEO Robin Li' s statement at the 2018 China Development Forum that "Chinese users are willing to trade privacy for convenience" [3], followed by JD.com' s price discrimination incident based on user consumption data [4], exposed the lack of transparency in data disposal by data owners and reflected Internet users' helplessness in privacy protection. These issues have gradually attracted social attention, with surveys revealing widespread public concern about APP privacy protection issues that significantly impact user behavior [5-7]. Account cancellation, as a means for personal information withdrawal, represents users' rights to control, dispose of, and dominate their personal information online. Although China has not explicitly defined a "right to cancellation," some legal systems and regulations

implicitly recognize users' account cancellation rights.

The EU's data protection regime, dating back to the 1970s, culminated in the adoption of the GDPR in April 2016—hailed as the "strictest data regulation in history" [32]. Building upon the previous Data Protection Directive (Directive 95/46/EC), the GDPR features broad coverage, strong uniformity, and severe penalties, representing a milestone in cybersecurity and compliance integration [33]. Its forward-looking design has profoundly impacted global data governance ecosystems [34]. The GDPR's comprehensive provisions on rights related to account cancellation have been widely accepted and implemented by tech giants including Google [35], Microsoft [36], and Amazon [37], serving as an important reference.

Due to legislative traditions, legal concepts, and social environments, the United States has more dispersed and ambiguous regulations related to the "right to be forgotten," often conflated with privacy rights, facing greater implementation resistance and controversy with a generally negative attitude [38]. Therefore, this paper focuses on reviewing Chinese legal systems and relevant EU GDPR provisions related to account cancellation to lay the foundation for subsequent institutional comparison and construction.

2. Legal Framework for User Account Cancellation in the Mobile Internet Environment

2.1 Relevant Chinese Legal Provisions

Network accounts today contain information not only closely connected to users personally but also possessing high commercial value and potential benefits, thus bearing attributes of both personality rights and property rights. User data constitutes not only users' virtual property but also a concentrated manifestation of users' data rights. Although Chinese law has not yet defined personal data rights or the "right to be forgotten" [39], some scholars consider them as extensions of privacy rights in the digital era [40]. Consequently, account cancellation rights in China are primarily based on privacy rights and personal information protection regulations, including direct and indirect protections.

Direct protection includes the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (December 28, 2012), which in Article 1 brings "electronic information capable of identifying citizens' personal identity and involving citizens' personal privacy" under state protection. Citizens have the right to demand network service providers delete relevant information or take other necessary measures to stop leaks of personal identity, dissemination of personal privacy, and commercial electronic information harassment. The Cybersecurity Law of the People's Republic of China, implemented on June 1, 2017, provides multiple protections for cybersecurity while further emphasizing users' control and decision-making power over personal data. Articles 22, 40, 41, 42, and 43 clearly limit net-

work operators' personal information usage behaviors, specifying that operators must obtain consent regarding the "purpose, method, and scope" of personal information use. Users who discover illegal or non-compliant use of their personal information have the right to demand its deletion. Such provisions demonstrate that users should have autonomous control over personal data information throughout its entire lifecycle from generation to extinction, and legally deleting personal information is an obligation that network operators must fulfill.

Indirect protection includes Article 38 of China's Constitution, which stipulates that citizens' personal dignity is inviolable; the Criminal Law, which criminalizes illegal acquisition, provision, or sale of personal information; Article 36 of the Tort Liability Law, which states that network users and service providers who infringe upon others' civil rights through networks shall bear tort liability; and Article 29 of the Consumer Rights Protection Law, which requires business operators collecting and using consumers' personal information to follow principles of legality, propriety, and necessity, and to adopt technical and other necessary measures to ensure information security and prevent leakage or loss. At the departmental regulation level, the Ministry of Industry and Information Technology's Provisions on the Protection of Personal Information of Telecommunications and Internet Users explicitly states in Chapter 2, Article 9 that telecommunications business operators and Internet information service providers shall stop collecting and using users' personal information after users terminate telecommunications services or Internet information services, and provide services for canceling numbers or accounts.

In summary, although China's current legal system lacks specialized personal privacy protection laws and explicit provisions directly related to user account cancellation, with relevant laws and regulations being relatively dispersed and simple, existing legal provisions indicate that users enjoy full rights to know and decide on personal information collection and use. Users can legally require network platforms to stop using and clean up personal information to prevent privacy leakage. Network operators must not only use user information within legal frameworks but also have obligations to provide account cancellation services, promptly stopping information mining and use after users terminate services to protect users' autonomous choice rights and the personality interests contained in personal information protection.

2.2 Relevant EU GDPR Provisions

In the mobile Internet environment, to help citizens better control and process personal information and prevent excessive collection and use, the EU formally proposed the concept of the "right to be forgotten" in 2012 [42] and first implemented it as an operational civil right in the 2014 Google v. González judgment [43]. The EU's 1995 Data Protection Directive already contained elements of the "right to be forgotten," with Article 6(1)(e) limiting data use to not exceed the original collection purpose, and Article 7 specifying particular circumstances for data processing, though Article 14 allows citizens to refuse data processing

for direct marketing purposes, and Article 12(b) explicitly states citizens have the right to "erase data processed in violation of this Directive" [44]. Building on this, the EU released the GDPR proposal in 2012 to update the "Directive 95/46/EC," with the most significant change being detailed provisions on the right to be forgotten' s subjects, obligors, and exercise conditions.

After years of discussion, the EU Commission officially adopted the GDPR in April 2016 to replace "Directive 95/46/EC," with the regulation taking effect on May 25, 2018. In terms of coverage, the regulation applies to any network sites and mobile APPs accessible and usable by individuals within the EU, meaning "the target users of the product or service include EU users," so overseas enterprises cannot be exempted. Regarding obligors, data controllers also include information dissemination controllers such as search engines, who must not only fulfill erasure obligations themselves but also notify other information controllers [43].

According to Article 4 of the GDPR, personal data refers to "any information relating to an identified or identifiable natural person (data subject)," encompassing names, ID numbers, location data, online identifiers, and even physical, psychological, genetic, cultural, or social aspects of natural persons, demonstrating broad coverage. Article 17 establishes the "Right to erasure," which has incorporated the separately listed "Right to be forgotten" from the draft. This article directly guarantees users' cancellation rights. Article 17(1) stipulates that user data shall be erased without undue delay when the collection purpose is no longer necessary, when processing is illegal, when users withdraw consent, or when erasure is required by member state law. Article 17(2) further states that if the controller has publicly disseminated personal data under Article 17(1), besides erasing it themselves, they should take technical measures to inform other data controllers to delete corresponding data links and copies, i.e., to stop third-party use of personal data. Article 17(3) specifies special circumstances for data retention, including that data erasure cannot hinder others' freedom of speech or harm national and public interests. Additionally, Article 21(2) continues the tradition of "Directive 95/46/EC," allowing users to refuse personal data being used for direct marketing purposes. The GDPR also imposes severe penalties for violations of the right to be forgotten, with Article 83(5) stipulating that data controllers who fail to comply with Article 17 requirements may face administrative fines up to €20 million or 4% of the enterprise' s annual global turnover.

Article 20 of the GDPR explicitly grants data subjects the "Right to data portability," which can help users better transfer data before or during account cancellation. In terms of scope, the right to data portability applies to personal data provided by data subjects to controllers based on explicit consent for specific purposes, as well as user data automatically generated during service provision, but excludes data collected from other sources or derived from secondary mining by data controllers [45]. In terms of data format, personal data obtained by data subjects should be structured, organized, machine-readable,

and in commonly used formats. Regarding usage purposes, data subjects have the right to transmit or migrate such data to another controller after obtaining it. The GDPR also stipulates that exercising the right to data portability must not affect the right to be forgotten under Article 17, and both rights do not apply to data processing conducted for public interest or official authority purposes, nor can they negatively impact others' rights or freedoms or legal obligations. Additionally, processing of certain special types of data may be permitted under special circumstances. Furthermore, Article 18 establishes the data subject' s "Right to restriction of processing" against controllers to limit processing activities.

The GDPR is a universal law for personal data protection that not only defines various roles and behaviors in data processing in detail but also emphasizes and expands data subjects'rights, particularly requiring data controllers'actions to be transparent and consented to by data subjects. Under the GDPR, data subjects have the right to terminate data services within legal limits and require data controllers or processors to delete or return data to effectively protect individual legitimate rights and interests. As the GDPR takes effect, its profound impact is gradually emerging, meaning users should have the right to cancel accounts and proactively retrieve or delete their personal information.

3. Comparison of Account Cancellation Mechanisms in Domestic and International Mobile Internet Apps

Domestic mobile Internet privacy research started later than abroad [26], and due to differences in legal systems, policy frameworks, social environments, and historical cultures [46], there are significant gaps between domestic and international account cancellation mechanisms in APP practices. Horizontal comparison helps identify problems for further improvement. Moreover, APPs with certain user scale and stable market share have more complete, practical, and reliable cancellation mechanisms, whose implementation will have broader and deeper impacts on relevant stakeholders. To enhance the generalizability of research conclusions, we referenced Apple App Store rankings from December 2018 for China' s and Europe' s top 100 downloaded apps and TOP5 data across various fields [47], selecting in January 2019 ten apps from different domains with over ten million users each for investigation. Domestic apps included social (WeChat, QQ, Weibo), shopping (Taobao, JD.com), transportation (Didi, Mobike), search (Baidu), payment (Alipay), and knowledge (Zhihu) categories. International apps included social (Skype, Facebook, LinkedIn), shopping (eBay, Amazon), transportation (Airbnb, Uber), search (Google), and payment (PayPal) categories. The research focused on user data obtained by apps before cancellation, prerequisites and processes during cancellation, and data retention after cancellation. According to GDPR' s jurisdictional scope, the ten selected international apps were verified to have high popularity in EU regions and have adjusted their policies to comply with GDPR requirements. Therefore, we conducted the international portion of the investigation from the perspective

of EU users and the domestic portion from the perspective of Chinese users to ensure research validity. Specific results are summarized in and .

Based on the practical survey results, we can compare and analyze the current cancellation status of domestic and international apps from the following aspects.

3.1 Difficulty of Registration and Cancellation

Overall, domestic APP accounts are relatively easy to register but difficult to cancel. Most APPs have simple registration processes that can be completed quickly through third-party authorization or even mobile phone verification. However, regarding cancellation, some service providers do not offer cancellation entry points, making account cancellation impossible, while others have relatively hidden cancellation entries with single channels and complicated prerequisites and terms, particularly for social and shopping apps. For example, Sina Weibo's cancellation requires meeting up to seven conditions, including "unbinding the Weibo account from other APP and website accounts" and "clearing external authorization relationships," without providing users with corresponding authorization or binding lists. Mobike requires users to provide "original ID card" and "photo holding the ID card" to verify identity. These conditions make cancellation time-consuming and fraught with obstacles.

International account registration and cancellation processes are relatively simple. Some foreign apps allow direct login using other large-scale Internet platform accounts like Microsoft or Google during first use, in addition to common username, password, email, or phone number registration. During cancellation, foreign service providers typically allow users to "delete accounts" through built-in APP options, making the process simpler than domestic counterparts. Apps like Airbnb, eBay, and LinkedIn only require checking a "cancellation reason," with options usually including "cannot meet needs" or "privacy and security concerns." Some authorized Internet platforms also provide associated account management centers; for example, Google allows users to quickly delete specific services like Gmail or YouTube. After users submit cancellation requests, social apps typically promise to retain user data for a certain period, with Skype, Facebook, and LinkedIn allowing users to restore or restart accounts during this period before data is sealed or deleted upon expiration.

3.2 Initiative in Account Cancellation

From the perspective of initiation subjects, account cancellation methods fall into two categories: user-initiated cancellation and service provider-initiated cancellation. In China, the initiative for cancellation is largely controlled by APP service providers, leaving users with limited options. Service providers universally treat account cancellation as an important measure to punish users who violate agreements or laws in their "service agreements" and "personal information protection policies" during registration. For example, WeChat stipulates

that Tencent has the right to "penalize account cancellation" for users violating service agreements. Some service providers have established account recovery mechanisms; NetEase Mail and Baidu both stipulate they can reclaim accounts with no activity for six consecutive months. This shows service providers have significant authority over account cancellation, but for user-initiated cancellation requests, most companies lack clear terms in registration agreements. Apps like Zhihu and Mobike require contacting human customer service for application and confirmation, with service providers holding final decision-making and interpretive power over whether to approve cancellation and able to terminate the cancellation process under special circumstances such as state organ investigations.

International apps emphasize users' account cancellation rights more strongly in their service and privacy terms, especially with adjustments and detailed modifications for the EU' s GDPR. Mandatory cancellation is mostly triggered when users violate laws, regulations, or terms and policies. Amazon stipulates users' rights to access, correct, and delete data, and provides channels for contacting third-party dispute resolution agencies and the "Privacy Shield" working group to help European users better realize data subject rights. Freezing or disabling accounts is also a common measure used by foreign APP service providers to maintain community health and service safety and comply with government department instructions to avoid legal risks and liabilities. Facebook and Twitter send freeze or disable notifications in such cases, allowing users to appeal, lift restrictions, or take other actions according to prompts.

3.3 Data Retention and Use by Service Providers After Cancellation

Domestic apps generally have opaque data clearing, retention, and subsequent use practices. All service providers explain and stipulate data obtained by apps in relevant privacy protection terms, with data mainly sourced from three categories: actively provided by users, generated during usage, and authorized by third parties. Most surveyed apps stipulate in service agreements that cancellation will clear "account-related information" while also stating that some information will be retained for a certain period. Domestic shopping apps not only obtain more types of data during use compared to foreign apps but also retain more user information upon cancellation. For example, Taobao stipulates that withdrawing consent "will not affect previous personal information processing based on your authorization," nor "immediately delete corresponding information from backup systems," meaning service providers retain some user data even after cancellation is completed. The "cancellation residue" problem is widespread, with "fake cancellations" that are only invisible to users occurring frequently. JD.com explicitly mentions in its Cancellation Notice that personal information is only removed from "front-end systems,"while "relevant transaction records" may be saved in back-end systems "for five years or even longer," and Baidu "can still retain relevant information before user cancellation." "Fake cancellation" is particularly evident in knowledge-based apps where user-generated

content is a core element; after Zhihu account cancellation, user-published content is not completely deleted and remains viewable, only showing the account as "banned," while "bound mobile numbers, emails, and third-party social accounts will not be automatically unbound and cannot be used to apply for new Zhihu accounts," creating obstacles for users' future use.

International apps have designed more complete user information retention mechanisms, providing download channels for account data including UGC data, personal profiles, and location data, and actively reminding users during cancellation to better preserve, access, and migrate data generated on the platform to prevent loss after cancellation. On Facebook's cancellation page, users can apply to download personal data including posts, chat records, profiles, and even ad clicks and login IPs; LinkedIn also allows users to download all personal information including articles, contacts, address books, and messages; Uber and Amazon also provide dedicated channels for obtaining user data copies. This data is converted into different machine-readable formats, compressed, and packaged for users to download within a certain period. Compared to domestic search app Baidu, Google, which also has a huge product ecosystem and complex account associations, has clearer and more scientific regulations. Before canceling an account, users can download data from over 30 Google-related products, and after archiving, receive download links via email to manage archive files online. More humanely, Google allows users to set up "inactive account management plans" to automatically trigger account deletion or share and send account-related content and data to designated contacts upon death or discontinuation of use.

3.4 Handling Third-Party Authorization During Cancellation

Registration through "data authorization" is becoming increasingly common. Large domestic authorization platforms like WeChat and Alipay have numerous data interfaces for third parties, but during cancellation, they shift the clearing responsibility to users, requiring users to unbind authorization relationships themselves without fulfilling the obligation to help users thoroughly and timely clear personal information. When cancellation is initiated in the authorized APP, due to lack of corresponding regulations on information processing by authorized platforms, whether the authorized APP can synchronously clear user data and links remains questionable, leaving hidden dangers for information leakage and malicious use.

International apps can also use social media platform accounts for direct login. Some apps, as branch applications or services under Internet giant systems without independent account systems (e.g., Bing can only use Microsoft accounts), have an "affiliated relationship" in data. When users log in, they agree to authorize branch applications to share user data with the original data holding platform, with branch applications acting as "data processors." Users cannot delete these branch application accounts separately and must operate through the authorizing account. For example, to delete a YouTube account logged in through Google, users can cancel YouTube service authorization in the Google

Account Management Center or cancel the connected Google account altogether.

Domestic apps in the user base expansion phase also provide login entrances using social media APP accounts, but these apps generally obtain user information through third-party authorization and further become actual data controllers, having a "parallel relationship" in data with the authorizing APP. After users log in with social media accounts, the APP automatically obtains information and creates an "independent account," usually requiring secondary binding with mobile phones or emails. In this case, cancellation operations must be performed separately in both the original and current apps; canceling only one party' s account does not mean the authorization relationship is unbound. Therefore, to thoroughly cancel, users must complete operations including unbinding third-party authorization and step-by-step cancellation.

International apps show relatively cautious and proactive attitudes in handling "parallel relationships" during cancellation. For example, Amazon states that third-party data use must also comply with its privacy protection obligations, and Amazon will be responsible for third-party inaction unless they can prove they are not responsible for data damage incidents. China is also showing similar trends.

3.6 Regional Differences in Cancellation Terms and Mechanisms

Domestic APP cancellation terms differ between domestic and overseas versions. Domestic mainstream apps like Alipay and WeChat have specific clauses for different regions in their international version service terms. For example, WeChat' s international version privacy policy explicitly defines users' account cancellation rights according to European law, provides data deletion appeal channels, and details processing methods and purposes, retention periods after cancellation for various user information types, and promises to "try to inform" third parties about "stopping personal information processing." Alipay' s overseas version "Alipay" privacy policy has "global" and "EU" versions, both explicitly allowing users to apply for personal information deletion. These foreign version clauses comply with and adapt to local regulations, with specific clauses taking precedence over general clauses.

Regional differences in foreign cancellation terms are more common. Comparisons reveal that foreign APP privacy terms also adjust according to the laws of the countries and regions where services are provided, or provide special services for specific regional users, especially in EU regions where the GDPR is implemented. For example, Airbnb manages user data through corresponding branch companies based on location and adopts different solutions and control levels according to regional laws and regulations. If users change their location, their data is transferred among data controllers in different regions, changing service relationships. When users submit cancellation requests, service providers fulfill corresponding obligations according to the laws and policies of users'current locations. Following GDPR provisions, European users can apply to access, update,

delete personal profiles or accounts at any time, and require APPs to respond and provide feedback promptly after verifying user identity. LinkedIn even provides EU users with privileged channels to completely erase personal data from the platform. APP service providers adopt regionally differentiated management measures to comply with mandatory requirements of different countries and to make cancellation settings meet various users' actual needs.

4. Full-Process Account Cancellation Mechanism in the Mobile Internet Environment

In summary, the GDPR has built a solid legal foundation for safeguarding user account cancellation from perspectives of scope of application, right to erasure, and right to data portability, and the cancellation status of apps has improved. However, numerous deficiencies persist, including complicated cancellation processes, service providers'rights exceeding their obligations, opaque data retention and use, imperfect follow-up mechanisms after cancellation, and incomplete handling of third-party authorization. In China, weak user information protection awareness, information abuse, and even black data industries pose enormous threats to user information security.

The key to solving current dilemmas lies in allowing user information to exit freely. Only through collaborative efforts among service providers, regulatory agencies, and users to build and improve a full-process account cancellation mechanism covering the complete lifecycle of user information can we truly standardize data processing behaviors, effectively protect user privacy and security, and eliminate users' worries. This paper defines the account cancellation mechanism as a standardized, modular, process-oriented, and comprehensive information management scheme and data processing system built based on corresponding legal provisions and technical standards to solve subsequent data clearing problems faced by information users during APP account cancellation, aiming to address information exit bottlenecks and contexts, clarify rights and responsibilities and relationships among multiple stakeholders, and protect user information rights and privacy. Therefore, starting from three stages—pre-cancellation, during cancellation, and post-cancellation—and drawing on GDPR concepts and practices, the implementation path for a full-process account cancellation mechanism in the mobile Internet environment can be designed according to the following three components.

4.1 Pre-Cancellation Safeguards

Smooth account cancellation must be based on sound institutional provisions. User agreements and privacy protection agreements of APP service providers should at least cover four aspects: data types, scope, usage purposes, application aspects, and processing methods obtained from users at different usage stages; rights and obligations of both service providers and users regarding account cancellation and relevant regulations to be followed; specific cancella-

tion processes and processing plans, retention purposes, and retention periods for different data types after cancellation; specific regulations and measures to ensure consistent multi-party data processing and help users thoroughly cancel accounts when APP service providers authorize third-party processors and controllers and transfer data to third parties.

Users need to carefully read, understand, and agree to relevant agreement terms during registration and develop good cancellation habits to reduce personal privacy leakage risks. In addition to users actively applying for account cancellation when no longer using relevant platforms, service providers should also be allowed to forcibly cancel accounts that endanger platform security or involve illegal activities according to relevant laws and regulations. In the mobile Internet environment, service providers should provide multiple account cancellation channels including APP clients, Web interfaces, human customer service, and email applications to ensure users can smoothly initiate cancellation requests.

Regulatory agencies must first clarify data processing plans for various APP account cancellations, including specific technical means, processing contexts and purposes, processing plans and scope, processing time limits, specific impacts on users, enterprises, and the state, and comprehensively assess associated risks to issue cancellation guidance opinions for APPs in different fields. Subsequently, through supervisory review of APP user agreements, they should ensure accuracy of rights provisions and rationality of specific clauses, helping APP service providers build account cancellation systems more scientifically and standardized.

4.2 Processing During Cancellation

Cancellation processing primarily revolves around service providers. The data they control includes not only data "actively" provided by users but also user profiles and third-party authorization data "passively" generated during usage, which depict user identities and behaviors from multiple dimensions. As shown in [Figure 2: see original paper], as the implementation subject of the account cancellation system, service providers must first formulate cancellation plans addressing three aspects during cancellation operations.

(1) **User-oriented data retention mechanism.** APP service providers should allow users to exercise the "right to data portability," proactively reminding users to selectively copy or back up personal data on the APP platform before cancellation, and providing accessible channels and file formats that facilitate user preservation, transmission, migration, and reuse. Consideration should be given to designing relevant tools to help users customarily download data to local storage, ensuring users' rights to migrate machine-readable data among different service providers without barriers.

(2) **Internal data classification processing mechanism.** According to regulatory guidance and the "data minimization" principle, service providers' processing methods for different data types should mainly fall

into three categories: First, complete erasure and forgetting. Most user data should be permanently cleared from service providers' servers and databases, with corresponding types and clearance deadlines reported to users. Second, time-limited retention. Due to national security and enterprise needs, data stability requirements, and other reasons, a small portion of data may be retained by service providers for a certain period, but they must inform users about retained data types, reasons, usage scope, retention period, and clearance time. Third, permanent retention. An extremely small portion of data may be permanently retained by service providers. In addition to providing corresponding information to users, such data must undergo strict anonymization processing, including deleting, replacing, or masking certain fields, randomly adding meaningless information, and irreversibly encrypting and de-identifying identity information.

(3) **Clearing response mechanism for third-party data controllers and processors.** For situations where service providers, with user consent, hand over user information to third parties for processing and preservation during usage, all data authorization association details should be disclosed to users, and users should be allowed to retain or withdraw authorizations. Authorizers should promptly notify third-party data subjects of the requirement to delete content, links, and other backup information related to user data through technical and automated measures, and request operational responses and result feedback to help users complete data deletion.

Integrating the above steps, service providers should provide users with a personal data deletion plan report, along with legal risk alerts and suggestions from internal data protection officers [48], and set a cooling-off period allowing users to withdraw cancellation requests and retain accounts. If users provide no feedback, account cancellation and corresponding data clearance operations are finally executed according to plan. The cancellation process and assessment are highly repeatable in a particular APP and should therefore be solidified into specific systems in practice and continuously optimized based on actual conditions.

Regulatory agencies must, on one hand, supervise whether service providers process user data in compliance with legal requirements, and review specific deletion and retention processes and results based on the data deletion plan report to prevent information abuse and illegal transfer. On the other hand, when discovering that data being processed endangers national stability, public safety, or is under administrative or judicial investigation, they have the right to terminate illegal account cancellation operations and retain and freeze corresponding data.

4.3 Post-Cancellation Protection

After completing actual operations, service providers should, within a certain time limit, produce special-format user account cancellation processing result reports based on facts to ensure the reports can be used as relevant evidence [49]. In addition to implementation records of service providers' data processing and protection measures, report content should also include processing feedback from third-party data controllers and processors. Data protection officers should clearly inform users of potential risks and legal issues that may still exist after cancellation completion and, where possible, provide contact information for users to consult and seek help. Finally, service providers should send complete cancellation processing result reports to users via email and other channels and archive them.

As shown in [Figure 3: see original paper], in addition to service providers themselves, data protection officers and regulatory agencies need to play greater roles, with the three parties jointly forming a closed loop for protecting user information security. Data protection officers, appointed by and responsible to enterprises, possess professional knowledge of data protection, information security law, and industry norms. They can assess the impact and risks of account cancellation from an enterprise perspective, provide professional consulting services, participate comprehensively in account cancellation operation processes, help enterprises build cancellation systems, conduct personnel and system training, evaluate relevant risks, and provide suggestions. They should also serve as a bridge between service providers and regulatory agencies.

Regulatory agencies need to review the legality and appropriateness of data processing after the fact based on relevant laws and regulations, comparing plan reports and result reports. They should use a combination of mandatory and non-mandatory means to regulate and correct improper behaviors of data controllers and processors, urge service providers to rectify or restart cancellation processes, and build dynamic regulatory mechanisms requiring service providers to conduct regular special reports to timely capture and identify new risk changes in data processing, achieving continuous and normalized regulation. Based on relevant implementation conditions, they should also provide guiding opinions. When data leakage and other security risks occur, especially involving personally identifiable information retained by service providers after account cancellation, data processors and controllers should activate emergency response mechanisms within specified time limits, report relevant facts to regulatory agencies and inform user subjects. Data protection officers should quickly intervene to assess situations and provide professional suggestions, while regulatory agencies should promptly guide relief actions, verify service providers' strict compliance with relevant regulations, and initiate accountability and penalty mechanisms afterward.

Additionally, regulatory agencies can regularly rate service providers' technical and organizational aspects of cancellation processing, issuing corresponding

level certifications based on process compliance, system completeness, personnel professionalism, and cancellation timeliness, and release information to the public in a timely manner.

References

[1] HASHEM I A T, YAQOOB I, ANUAR N B, et al. The rise of "big data" on cloud computing: review and open research issues [J]. Information systems, 2015, 47: 98-115.

[2] LUTZ C, HOFFMANN C P, BUCHER E, et al. The role of privacy concerns in the sharing economy [J]. Information, communication & society, 2018, 21(10): 1472-1492.

[3] CCTV News. Commentary: Who said "Chinese people are willing to trade privacy for convenience"? [EB/OL]. [2018-12-28]. http://news.163.com/18/0328/03/DDV513QI0001875N.html

[4] Zhihu. How to evaluate JD.com' s price discrimination? [EB/OL]. [2018-12-28]. https://www.zhihu.com/question/270660676.

[5] GU J, XU Y C, XU H, et al. Privacy concerns for mobile app download: an elaboration likelihood model perspective [J]. Decision support systems, 2017, 94: 19-28.

[6] JUNG Y, PARK J. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services [J]. International journal of information management, 2018, 43: 15-24.

[7] WOTTRICH V M, VAN REIJMERSDALE A, SMITE G. The privacy trade-off for mobile app downloads: the roles of app value, intrusiveness, and privacy concerns [J]. Decision support systems, 2018, 106: 44-52.

[8] Backgroundchecks. A directory of direct links to delete your account from web services [EB/OL]. [2018-12-28]. https://backgroundchecks.org/justdeleteme/.

[9] BRANDTZAEG P B, PULTIER A, MOEN M. Losing control to data-hungry apps: a mixed-methods approach to mobile app privacy [J/OL]. Social science computer review, 2018: 1-23. [2019-04-29]. https://doi.org/10.1177/0894439318777706.

[10] DEV MANE M A, RANA N K. Privacy issues in online social networks [J]. International journal of computer applications, 2012, 41(13): 5-8.

[11] HERRMANN D, LINDEMAN J. Obtaining personal data and asking for erasure: do app vendors and website owners honour your privacy rights? [EB/OL]. [2019-04-29]. https://arxiv.org/abs/1602.01804.

[12] BAUMER E P S, ADAMS P, KHOVANSKAYA V D, et al. Limiting, leaving, and (re)lapsing: an exploration of Facebook non-use practices and experiences [C]//Proceedings of the SIGCHI conference on human factors in computing systems. New York: ACM, 2013: 3257-3266.

[13] LOCASTO M E, MASSIMI M, DEPASQUALE P J. Security and privacy considerations in digital death [C]//Proceedings of the 2011 new security paradigms workshop. New York: ACM, 2011: 1-10.

[14] EU. General data protection regulation [EB/OL]. [2018-12-29]. https://gdpr-info.eu/art-20-gdpr/.

[15] POLITOUE E, ALEPIS E, PATSAKIS C. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions [J]. Journal of cybersecurity, 2018, 4(1): 1-20.

[16] China Consumer Association. Evaluation report on personal information collection and privacy policies of 100 apps [EB/OL]. [2018-12-28]. http://www.cca.org.cn/jmxf/detail/28310.html?tdsourcetag=s_{{{pctim}}}_{{aiomsg}}}.

[17] Information and Communication Administration. MIIT' s Information and Communication Administration interviews relevant enterprises on strengthening user personal information protection [EB/OL]. [2018-12-28]. http://www.miit.gov.cn/n1146290/n4388791/c6010832/content.html.

[18] CCTV News. Mobile APP accounts difficult to cancel—MIIT: cancellation services must be provided [EB/OL]. [2018-12-29]. http://www.xinhuanet.com/tech/2018-01/05/c_{1122213028}.htm.

[19] Ministry of Industry and Information Technology. MIIT notice on telecommunications service quality (No. 4 of 2018) [EB/OL]. [2018-12-28]. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c6471882/content.html.

[20] ANTIGNAC T, SCANDARIATO R, SCHNEIDER G. A privacy-aware conceptual model for handling personal data [C]//International symposium on leveraging applications of formal methods. Cham: Springer International Publishing, 2016: 942-957.

[21] FAWAZ K, SHIN K G. Location privacy protection for smartphone users [C]//Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. New York: ACM, 2014: 239-250.

[22] SUNYAEV A, DEHLING T, TAYLOR P L, et al. Availability and quality of mobile health app privacy policies [J]. Journal of the American Medical Informatics Association, 2014, 22(e1): e28-e33.

[23] KOKOLAKIS S. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon [J]. Computers & security, 2017, 64: 122-134.

[24] GOLBECK J, MAURIELLO M. User perception of Facebook app data access: a comparison of methods and privacy concerns [J/OL]. [2019-05-13]. https://doi.org/10.3390/fi8020009.

[25] CHOI B C F, LAND L. The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage [J]. Information & management, 2016, 53(7): 868-877.

[26] WANG X W, XIANG M M, ZHANG C L, et al. Research trends in information privacy under new media environment at home and abroad [J]. Library and information service, 2017, 61(15): 6-14.

[27] WANG H, ZHANG L. Research on network privacy protection model for personal information management [J]. Information science, 2015, 33(10): 47-51.

[28] SHEN H Z, TANG X T, ZHOU Y. Usability study of privacy protection functions in domestic mobile social media [J]. Library and information service, 2017, 61(4): 23-30.

[29] TIAN B, ZHENG Y S, LIU P Y, et al. Risk evaluation index system and empirical research on mobile APP user privacy information leakage [J]. Library and information service, 2018, 62(19): 101-110.

[30] ZHANG Y, WANG J, ZHU Q H. Research on influencing factors of user cognition of medical APP privacy policies based on grounded theory [J/OL]. [2019-05-17]. http://kns.cnki.net/kcms/detail/11.1762.G3.20190122.1424.004.html.

[31] ZHANG L A, HAN X Z. "Right to be forgotten" : new issues in the big data era [J]. Hebei law science, 2017, 35(3): 35-51.

[32] CHANG N. Impact and countermeasures of EU General Data Protection Regulation [J]. China information security, 2018(6): 90-93.

[33] ZERLANG J. GDPR: a milestone in convergence for cyber-security and compliance [J]. Network security, 2017, 2017(6): 8-11.

[34] WU S H. EU General Data Protection Regulation (GDPR) and China' s response [J]. Information security and communications privacy, 2018(6): 13-16.

[35] Google. We are committed to complying with applicable data protection laws [EB/OL]. [2018-12-08]. https://privacy.google.com/businesses/compliance/.

[36] Microsoft. Safeguard individual privacy with the Microsoft Cloud [EB/OL]. [2018-12-08]. https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview.

[37] Amazon. General data protection regulation (GDPR) center [EB/OL]. [2018-12-08]. https://aws.amazon.com/cn/compliance/gdpr-center/.

[38] YU X H. Research on the right to be forgotten [D]. Changchun: Jilin University, 2018.

[39] ZHOU D. Research on civil law protection of personal data in the big data era [D]. Wuhan: Central China Normal University, 2015.

[40] LI W L. Privacy protection and right to be forgotten in the big data era [D]. Beijing: China University of Political Science and Law, 2015.

[41] Xinhua News Agency. Decision of the Standing Committee of the National People' s Congress on strengthening network information protection [EB/OL]. [2018-12-28]. http://www.gov.cn/jrzg/2012-12/28/content_{2301231}.htm.

[42] REDING V. The EU data protection reform 2012: making Europe the standard setter for modern data protection rules in the digital age [C]//USA: Innovation conference digital, life, design munich. 2012, 22.

[43] HU X. Legal construction of the right to be forgotten system [D]. Wuhan: Central China Normal University, 2017.

[44] YANG L X, HAN X. Localization and legal application of the right to be forgotten in China [J]. Law application, 2015(2): 24-34.

[45] CAO Y T. Preliminary exploration of the right to data portability and its impact on credit industry [J]. Credit reference, 2016, 34(9): 26-28.

[46] COCKCROFT S, REKKER S. The relationship between culture and information privacy policy [J]. Electronic markets, 2016, 26(1): 55-72.

[47] Apple. App store rankings [EB/OL]. [2018-12-09]. https://www.apple.com/itunes/charts/free-apps/.

[48] WAN L. Concepts, responsibilities, and competency of foreign personal data protection officers [J]. Library and information service, 2018, 62(17): 129-135.

[49] XIAO D M, TAN L G. EU data protection impact assessment system and its implications [J]. Journal of the China Society for Scientific and Technical Information, 2018, 44(5): 76-86.

Author Contributions

Wu Renli: Proposed the research framework, wrote and revised the paper, designed the cancellation mechanism diagrams.

Wu Shuqian: Collected materials and translated English content, wrote the paper, drew the cancellation mechanism figures.

Note: Figure translations are in progress. See original paper for figures.