Regulating Bundled Consent in Digital Services

Yang Jianing[1]*

[1] Henan University of Economics and Law, Zhengzhou 450046, China
* Correspondence: 3336965212@qq.com

https://doi.org/10.53104/curr.res.law.pract.2026.03001

Citation: Yang, J. (2026). Regulating Bundled Consent in Digital Services. *Current Research in Law & Practice*, *4*(1), 1-10.

Abstract: Bundled consent is a common problem in digital services. Users are often asked to accept several data processing activities through one general consent button, including account registration, personalized recommendation, marketing, and third-party sharing. Although this form of consent appears lawful, it may weaken users' real choice when necessary and non-essential processing are tied together. Based on the legal principles of informed consent, necessity, separate consent, and the right to withdraw consent, this paper examines how bundled consent should be regulated. It argues that the law should not focus only on whether users have clicked "agree," but should also consider whether consent is voluntary, specific, separable, and easy to withdraw. Digital service providers should distinguish necessary authorization from optional authorization, provide clearer notices, and allow users to refuse non-essential processing without losing access to basic services.

Keywords: bundled consent; personal information processing; digital services; informed consent; user autonomy

1. The Problem of Consent in Everyday Digital Services

Consent has become one of the most familiar legal gestures in digital life. A user opens an app, registers an account, enters a platform service, or uses a mini-program, and a privacy policy or authorization window appears before the service can continue. In form, the platform has asked for permission. The user has also clicked "agree." Yet this familiar process does not always mean that the user has made a real choice.

The problem is more visible when digital services become part of ordinary social life. According to the 57th Statistical Report on China's Internet Development, the number of internet users in China reached 1.125 billion by December 2025, with an internet penetration rate of 80.1%. Online shopping users reached 937 million (China Internet Network Information Center, 2026). These figures show that privacy authorization is no longer an occasional legal act. It is repeated in shopping, payment, travel, communication, entertainment, learning, and many other services. Users face consent requests so often that clicking "agree" easily becomes a habit rather than a careful decision.

Bundled consent grows out of this setting. Many platforms do not ask users to consent to one clear processing activity. Instead, they place several matters together: account registration, device

permissions, personalized recommendation, marketing messages, user profiling, and possible third-party sharing. These matters may have different purposes and different degrees of necessity, but they are often presented through one general button. The user is not asked to decide separately. The choice is usually simplified into acceptance or exit.

This does not mean that all integrated privacy notices should be treated as unlawful. Digital services do need certain personal information to operate. A shopping platform may need delivery information. A payment service may need identity verification. A navigation service may need location information. The difficulty lies elsewhere. Some platforms use the entrance to a necessary service to obtain permission for additional processing that is not truly required for the basic function. In such cases, consent becomes broader than the service itself.

For this reason, the legal question should not stop at whether the user has clicked "agree." A more important question is whether the user had a meaningful chance to understand and refuse non-essential processing. If refusal means losing access to the basic service, or if different processing purposes are hidden under one consent button, the autonomy protected by consent is weakened. Bundled consent therefore turns a rule designed to protect personal choice into a formal step in platform operation.

This paper starts from this tension between formal consent and meaningful choice. It examines when bundled consent in digital services should be legally questioned, and how the law can prevent consent from becoming only a procedural cover for excessive personal information processing.

2. The Forms of Bundled Consent in Digital Services

Bundled consent does not appear in only one fixed form. In digital services, it is often hidden in ordinary interface design. The user may see a privacy policy, a user agreement, or a pop-up window, but behind one consent button there may be several different data processing activities. These activities are not always equally necessary for the service. Some are closely connected with the basic function. Others serve advertising, user profiling, commercial cooperation, or future business use.

One common form is the bundling of necessary and non-essential processing. A platform may need certain personal information to provide the service. For example, a shopping service needs a delivery address, and a payment service may need identity or transaction information. But the same consent interface may also include personalized advertising, marketing messages, device information collection, or sharing with business partners. The user is not given a separate option to accept the basic service while refusing these additional activities. This kind of design makes the scope of consent much wider than the actual service need.

Another form is the bundling of different processing purposes. The platform may collect the same type of personal information for several purposes at once. Location information, for instance, may be used to provide nearby services, improve recommendation accuracy, analyze user behavior, or support advertising placement. These purposes are not the same in legal meaning. Some may be directly related to the user's request, while others mainly serve the platform's commercial interest. If they are placed under one broad consent clause, the user cannot know which purpose is necessary and which is optional.

Bundled consent may also appear in the treatment of sensitive personal information. Sensitive personal information usually requires more careful handling because misuse may cause greater harm to personal dignity, property safety, or personal safety. In practice, however, some services place sensitive information authorization together with ordinary information authorization. The user may not notice that the consent involves face recognition, precise location, financial account information, or other sensitive data. Once these matters are hidden inside a general consent process, the special protection required for sensitive information is weakened.

A further form is the bundling of platform service and third-party sharing. Many digital services are not provided by one single operator. Advertising partners, payment institutions, logistics providers, data analysis tools, and embedded SDKs may all take part in the service structure. Users usually do not have enough knowledge about these background arrangements. When a platform asks users to agree to "necessary cooperation with third parties" in a general clause, it may become difficult for users to know who will receive their information, for what purpose, and under what limits.

There is also a stronger form of bundled consent in the "agree or leave" structure. In this situation, the user is told that the service cannot be used unless all terms are accepted. The platform may not directly say that every item is compulsory, but the interface leaves no real path for partial refusal. The user cannot reject marketing, profiling, or non-essential permissions while continuing to use the basic function. This design is especially problematic when the service has become important for daily life, work, study, or social interaction.

These forms show that bundled consent is not simply a problem of long privacy policies. It is a problem of how choices are arranged. The platform may formally disclose many matters, but if different processing activities are tied together, the user's decision becomes unclear. The legal concern is not that digital services use personal information. The real concern is that users are asked to give one broad consent for matters that should have been separated.

3. The Impact of Bundled Consent on Personal Information Rights

Bundled consent affects personal information rights in a quiet but substantial way. It does not always look like a direct violation. The platform may have displayed a privacy policy, provided a consent button, and recorded the user's agreement. From the outside, the process seems complete. The difficulty is that the user's rights may already have been weakened before the click is made. When several processing activities are tied together, consent may lose its function as a tool of personal control.

The first impact is on the right to be informed. In personal information processing, notice is not only a formal step. It should help users understand what information will be collected, why it will be used, whether it will be shared, and what consequences may follow. Bundled consent makes this harder. Different purposes, different types of information, and different recipients may be placed in one long document or one general authorization page. Users can see that there is a privacy policy, but they may not be able to identify the matters that truly affect their rights.

This problem is not only caused by users' unwillingness to read. Privacy notices are often written in a technical and general way. Some clauses use broad expressions such as improving service quality, ensuring transaction security, providing personalized experience, or cooperating with third parties. These expressions are not meaningless, but they are often too wide to guide user choice. When the language is broad and the consent is bundled, the user cannot easily tell which part is necessary and which part is optional. The right to be informed is then reduced to being shown a document.

Bundled consent also weakens the user's right to make an autonomous decision. Consent should mean that the user can say yes or no to a specific processing activity. In many digital services, however, refusal is costly. A user may have to give up the entire service simply because he or she does not accept some non-essential processing. This is not the same as a free choice. The user may still click "agree," but the decision is made under pressure created by the service structure.

The pressure is stronger where digital services are closely connected with daily life. Online shopping, mobile payment, transport services, social communication, online learning, and medical appointment platforms are no longer optional in a simple sense. They are part of ordinary social participation. If a platform ties basic service access to broad data authorization, the user may have little practical room to refuse. In this situation, bundled consent turns the user's dependence on digital

services into the platform's advantage in obtaining data.

Another impact concerns the right to limit personal information processing. The principle of necessity requires that personal information processing should not go beyond what is needed for the stated purpose. Bundled consent tends to blur this boundary. Once the platform receives broad authorization, it may treat the user's agreement as covering many later uses. Data collected for registration may be used for profiling. Information provided for service delivery may later support recommendation, marketing, or risk assessment. The user may not clearly know when the original purpose has been exceeded.

This also increases the risk of excessive collection. A platform that asks for several permissions at the same time may collect more information than the user expected. The user may agree to location access for one function, but the platform may use location data to improve advertising or analyze behavioral patterns. The user may provide basic identity information for account security, but the platform may connect it with consumption habits, browsing records, and device identifiers. The harm here is not always immediate. It lies in the gradual expansion of data use.

Bundled consent further affects the right to withdraw consent. In theory, users should be able to change their decision after giving consent. In practice, withdrawal is often much harder than agreement. The consent button is placed at the entrance of the service, while the withdrawal path may be hidden in several layers of settings. Even when users find the option, they may not know which processing activity will stop and which will continue. If all consent has been bundled at the beginning, later withdrawal also becomes unclear.

The problem becomes more serious when withdrawal is linked to service restriction. Some platforms may allow withdrawal in form, but warn users that certain functions will become unavailable. This may be reasonable when the withdrawn information is truly necessary for the function. It is less reasonable when the user only refuses marketing, profiling, or non-essential sharing. If withdrawal of non-essential consent leads to a loss of basic service, the right to withdraw exists only on paper.

Bundled consent may also affect equality between users and platforms. Platforms design the interface, draft the privacy policy, decide the technical path, and control access to the service. Users usually face these arrangements individually. They lack the information, time, and bargaining power to negotiate different data processing terms. This imbalance does not make every consent invalid, but it explains why the law should not treat a click as conclusive evidence of free choice.

The impact of bundled consent is therefore not limited to one single right. It weakens informed consent, reduces user autonomy, expands the possibility of excessive processing, and makes withdrawal more difficult. These effects are connected. When users do not understand the scope of processing, they cannot make a real choice. When they cannot make a real choice, the scope of processing becomes easier to expand. When the scope expands, later withdrawal becomes harder. This is why bundled consent should be examined as a structural problem in digital services, not merely as a drafting defect in privacy policies.

4. The Legal Basis for Controlling Bundled Consent

The legal control of bundled consent does not require the creation of a completely new rule. Existing rules on personal information protection already provide a basis for examining this problem. The difficulty is that bundled consent often looks lawful at the surface level. The platform gives notice, the user clicks agree, and the system records consent. If the review stops there, many problems will be missed. The law therefore needs to look at the quality of consent, not only at the existence of a consent button.

A useful starting point is the requirement of informed and voluntary consent. Consent in personal information processing should be made after the user has received enough information and

has a real chance to decide. This requirement is not satisfied merely because a privacy policy exists somewhere in the service interface. If the notice is too general, too long, or too difficult to understand, the user may not know what he or she is agreeing to. In bundled consent, this problem is common because several purposes and several types of information are mixed together. The user sees one agreement, but the actual processing activities behind it may be much wider (Standing Committee of the National People's Congress, 2021).

The principle of necessity is more directly related to bundled consent. Personal information processing should be limited to what is necessary for the stated purpose. This principle helps separate basic service needs from additional commercial interests. A digital service may need some personal information to function. But it does not follow that the platform can use the same service entrance to obtain consent for advertising, profiling, unnecessary device permissions, or broad third-party sharing. Once non-essential processing is tied to basic service access, the consent begins to lose its voluntary character.

The *Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications* provide a clearer way to understand necessity. These provisions define necessary personal information as the information without which the basic function of an app cannot operate. They also state that an app should not refuse to provide its basic function merely because the user does not agree to provide non-essential personal information. This rule is important for bundled consent. It means that the platform cannot simply treat all requested information as a condition for using the service. The basic function and the additional processing should be separated (Cyberspace Administration of China et al., 2021).

The *Methods for Identifying Illegal Collection and Use of Personal Information by Apps* also provide practical standards. They identify several problematic practices, such as collecting personal information before consent is obtained, continuing to collect information after the user refuses, using default consent, frequently asking for consent in a way that interferes with normal use, collecting information beyond the authorized scope, and failing to provide a way to withdraw consent (Cyberspace Administration of China et al., 2019). These standards do not use the expression "bundled consent" as the central concept, but they describe many of its concrete forms.

These regulatory rules are valuable because they shift attention from formal agreement to actual choice. For example, if an app asks users to open several permissions at once and refuses service when users disagree, the problem is not only that the privacy notice is unclear. The deeper problem is that the user is not allowed to separate necessary authorization from unnecessary authorization. If an app says that data will be used to "improve service quality" or "provide better user experience," but forces the user to accept broad collection, such wording cannot by itself justify the scope of processing.

Separate consent is another important basis. Certain processing activities involve greater risks, such as the processing of sensitive personal information or the provision of personal information to another processor. These matters should not be hidden inside a general consent package. They require a more specific expression of the user's will. In bundled consent, however, sensitive information, third-party sharing, and ordinary service information may be placed together. This weakens the protective function of separate consent and makes high-risk processing look like part of ordinary service use.

The right to withdraw consent also supports the control of bundled consent. If consent can be given through one click but withdrawal is difficult, consent becomes unequal in practice. Users may not be able to identify which part of their consent they want to withdraw. They may also find that withdrawal of one authorization affects the whole account or the whole service. A valid consent system should allow users to change their decision in a reasonably convenient way. This is especially

important when the original consent was broad and bundled.

Consumer protection rules may also be relevant. In digital services, users are not only data subjects but also consumers. They often accept standard terms drafted by platforms in advance. They cannot negotiate the content of privacy policies or data processing terms. If a platform uses its stronger position to expand data collection through unclear or bundled terms, the issue is connected with fairness in online transactions. The user's personal information is not only a technical resource for the platform. It is also part of the user's personal rights and interests.

The existing legal framework therefore provides several points of control: clear notice, voluntary consent, necessity, separate consent, refusal of non-essential processing, and convenient withdrawal. These rules are already enough to question many forms of bundled consent. The real task is to apply them more carefully. A platform should not be allowed to rely on one general consent button when the processing activities behind that button have different purposes, different risks, and different degrees of necessity.

5. The Standards for Identifying Problematic Bundled Consent

The identification of problematic bundled consent cannot depend only on the outward form of consent. If the user has clicked "agree," it may show that a procedural step has been completed, but it does not necessarily prove that the consent is informed, voluntary, and specific. In digital services, the more important issue is how the consent was obtained. The law should therefore examine the structure of the consent mechanism, the relationship between the requested information and the service, and the degree of real choice left to the user.

A useful standard is service necessity. Personal information processing should be connected with the function that the user actually requests. Some information is clearly necessary. A shopping service needs delivery information. A payment service may need transaction and identity information. A navigation service may need location information. But this does not mean that the platform can require every type of data in the same consent process. If user profiling, marketing messages, personalized advertising, or unrelated third-party sharing is tied to basic service access, the consent should be treated with caution.

This standard is important because bundled consent often hides non-essential processing behind necessary service needs. The platform may claim that all requested information is used to improve the user experience or provide better services. Such language is too broad. It does not prove that the information is necessary for the basic function. The more distant the connection between the data processing activity and the service requested by the user, the more difficult it is to justify bundled consent.

The case of Luo v. A Technology Company shows this point clearly. The service provider required users to submit profiling information during the first login, including information related to user characteristics and learning needs. The company argued that the information was needed for recommendation services. Yet the problem was that such information was not necessary for basic access to the online service, and the user was not given another way to log in without submitting it. This case shows that a platform cannot simply label profiling as a basic function and then use that label to avoid the requirement of genuine consent. If the user must provide non-essential information before entering the service, the consent is not truly voluntary (Supreme People's Court, 2025b).

At the same time, service necessity should not be understood too narrowly. Not every collection of personal information beyond account name and password is unlawful. The case of Huang Mouhuan v. A Credit Management Company is useful as a comparison. In that case, the processing of certain credit-related information was connected with a "use first, pay later" service. The court accepted that such information processing was necessary for the selected function, because the service itself depended on credit assessment and risk control.

This case suggests that the legality of consent should be judged in relation to the specific service chosen by the user. If the information is genuinely needed for that function, the legal assessment will be different (Supreme People's Court, 2025a).

The second standard is separability of choice. Problematic bundled consent usually appears when users cannot make separate choices for different processing purposes. A single consent button may cover registration, service use, personalized recommendation, marketing, sensitive information processing, and third-party sharing. This arrangement is convenient for the platform, but it makes the user's decision unclear. The user may want to use the basic service, but may not want to accept marketing or profiling. If the interface does not allow this distinction, consent becomes too broad.

Separability is not a technical luxury. It is part of meaningful consent. Where different processing activities have different purposes and different risks, they should not be treated as one package. A platform should at least separate necessary processing from optional processing. It should also separate ordinary personal information from sensitive personal information, and separate internal service use from external sharing. The user should be able to agree to one matter without being forced to agree to all.

The third standard is the clarity of notice. Even where the platform gives users a choice, that choice may still be weak if the notice is unclear. A privacy policy may be formally complete but practically unreadable. It may be too long, too technical, or filled with vague expressions. In bundled consent, unclear notice creates a stronger problem because users must understand several processing activities at once. If important matters are hidden in general clauses, the user cannot know what is really being accepted.

Clear notice does not mean that every legal detail must be placed on the first screen. That may only make the interface more confusing. A better approach is layered notice. Basic information should be presented in a direct and readable way. Important matters, such as sensitive personal information, third-party sharing, automated decision-making, and marketing use, should be highlighted. Detailed rules can be placed in the full privacy policy, but key risks should not be buried there. If the platform wants to rely on consent, it should make the consent understandable.

Another standard is the availability of refusal without losing the basic service. This is often the point where bundled consent becomes most serious. If a user refuses non-essential processing and is then prevented from using the basic function, the refusal option is not meaningful. The user is placed in an "accept all or leave" position. This is different from a situation where refusal makes a specific function unavailable because that function truly depends on the information. The legal issue is whether the restriction is proportionate to the refused data processing.

For example, if a user refuses to provide a delivery address, an online shopping platform may be unable to complete a physical delivery order. That restriction is understandable. But if the user refuses personalized advertising and the platform blocks access to ordinary browsing or account login, the restriction is harder to justify. The same logic applies to marketing messages, broad device permissions, or unrelated data sharing. Non-essential processing should not become a hidden condition for basic service use.

The ease of withdrawal should also be considered. Consent is not only about the moment of agreement. It also includes the user's later ability to change the decision. Bundled consent makes withdrawal difficult because the original authorization is not separated. Users may not know which consent they are withdrawing, what data processing will stop, and whether the service will be affected. If the platform allows one-click consent but requires many steps to withdraw, the system favors data collection over user control.

A valid withdrawal mechanism should be visible, understandable, and not unnecessarily burdensome. The platform should not hide withdrawal options deep in account settings. It

should not make users contact customer service for matters that could be handled through the interface. It should also avoid using vague warnings to discourage withdrawal. If withdrawal of optional processing is made inconvenient, the earlier consent should not be treated as fully reliable.

The level of risk should be another factor. Some forms of bundled consent are more harmful than others. Where sensitive personal information is involved, the platform should face a higher standard. Information such as biometric data, precise location, financial account information, health information, and information concerning minors may cause serious harm if misused. These matters should not be absorbed into a general agreement. The higher the risk, the stronger the need for separate notice and separate consent.

Third-party sharing should also be judged carefully. Users may understand that the platform itself needs some information, but they may not expect that the information will be provided to other parties. In many digital services, SDKs, advertising partners, payment institutions, logistics companies, and data analysis providers may all be connected with the service. The platform should not use a broad clause to cover all such transfers. It should explain the type of recipient, the purpose of sharing, the category of information, and the user's available rights. Where the user cannot identify the outside recipient or the purpose of sharing, consent becomes weak.

These standards show that problematic bundled consent is not identified by one single factor. It should be assessed through the whole consent structure. The central questions are simple but important. Is the requested information necessary for the service? Can the user separate basic service consent from optional processing? Is the notice clear enough to support a real decision? Can the user refuse non-essential processing without losing basic access? Can the user withdraw consent in a practical way? Are sensitive information and third-party sharing handled with special care?

The comparison between Luo v. A Technology Company and Huang Mouhuan v. A Credit Management Company also shows that legal control should be balanced. The law should not deny all data processing in digital services. Some processing is indeed necessary for contract performance and service operation. But the law should also prevent platforms from expanding the idea of necessity too far. The decisive point is not whether the platform finds the information useful. The decisive point is whether the information is genuinely required for the function chosen by the user, and whether the user is given a real choice over matters beyond that function.

For this reason, the standard for identifying problematic bundled consent should move from formal consent to substantive choice. A consent mechanism is problematic when it uses one general agreement to cover different purposes, hides non-essential processing behind basic service needs, makes refusal unrealistic, or makes withdrawal difficult. In these situations, the user's click should not be treated as enough. The law should ask whether the consent was specific, separated, understandable, and reversible. Only then can consent continue to serve its proper role in personal information protection.

6. From Formal Consent to Meaningful Choice

The regulation of bundled consent should not be understood as a rejection of consent. Consent remains an important legal basis for personal information processing. The real problem is that consent has often been reduced to a formal procedure in digital services. A user clicks "agree," the platform records the action, and the processing begins. This process may be efficient, but efficiency alone cannot prove that user autonomy has been respected.

A better approach is to move from formal consent to meaningful choice. Meaningful choice does not require users to read every technical clause or negotiate every term with the platform. That would be unrealistic. It means that users should at least be able to understand the main processing activities, distinguish necessary processing from optional processing, refuse non-essential items, and withdraw consent without unreasonable difficulty.

These requirements are not excessive. They are the basic conditions that allow consent to retain its legal value.

Digital service providers should first separate necessary authorization from optional authorization. Information that is necessary for the basic function may be requested at the entrance of the service. For example, a shopping service may request delivery information when the user needs goods to be delivered. A payment service may request identity or transaction information when it is needed for payment security. But advertising, commercial marketing, personalized recommendation, user profiling, and broad third-party sharing should not be placed in the same compulsory consent package. These activities should be presented as separate choices.

This separation also helps avoid the overuse of the word "necessary." Platforms often describe many forms of data processing as necessary for better service, improved experience, or transaction security. Some of these reasons may be valid, but they should not be accepted too easily. Necessity should be judged by the basic function selected by the user, not by the platform's general business interest. If the service can still operate without a certain processing activity, that activity should not be treated as a condition for basic access.

The second step is to make notice clearer. Privacy notices should not only be legally complete; they should also be readable. A long privacy policy may protect the platform from formal criticism, but it may not help users understand their rights. Important matters should be placed where users can see them. Sensitive personal information, third-party sharing, automated decision-making, personalized marketing, and withdrawal methods should be highlighted in plain language. The full privacy policy can still provide detailed rules, but key information should not be buried in a long document.

Layered notice may be a more suitable method. The first layer can give users the most important information in a short form. The second layer can explain specific processing activities. The full policy can then provide detailed legal terms. This structure is more realistic than expecting users to read a long policy before every click. It also makes the platform explain its data practices more carefully.

The third step is to protect the right to refuse. Refusal should not be only a symbolic option. If users refuse non-essential processing, they should still be able to use the basic function where that function does not depend on the refused information. The *Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications* provide an important reference here. They make clear that apps should not deny basic services merely because users refuse to provide non-essential personal information. This rule directly responds to the "agree or leave" structure often seen in bundled consent.

The fourth step is to make withdrawal practical. Consent is not a one-time event. Users may change their minds after they understand more about the service or after their needs change. The withdrawal path should be easy to find and easy to operate. Platforms should not make withdrawal far more difficult than consent. Nor should they use unclear warnings to pressure users into keeping unnecessary authorization. If users can agree with one click but must go through several hidden pages to withdraw, the consent system is not balanced.

Regulatory enforcement also has a role. The Ministry of Industry and Information Technology has repeatedly issued notices on apps and SDKs that infringe user rights. These notices show that problems such as excessive permission requests, unclear authorization, and irregular personal information collection still appear in practice. Such enforcement should continue to focus not only on whether a privacy policy exists, but also on whether users are given real control over non-essential processing (Ministry of Industry and Information Technology, 2026).

For high-frequency digital services, regulators may need more detailed review standards. Services involving mobile payment, online shopping, transportation, learning, medical appointments, social communication, and financial functions have

stronger effects on daily life. In these areas, users are more likely to accept broad consent because they need the service. The more dependent users are on the service, the more carefully bundled consent should be examined.

Judicial review can also help clarify the boundary. Luo v. A Technology Company shows that requiring users to submit non-essential profiling information without an alternative login path may undermine voluntary consent. Huang Mouhuan v. A Credit Management Company shows, at the same time, that some processing may be justified when it is genuinely necessary for the selected service. These cases are useful because they do not treat all data processing as suspicious. They ask a more precise question: whether the information is truly needed for the service and whether the user has been given a real choice.

The final goal is not to make digital services impossible to operate. Platforms need personal information to provide many services. Users also benefit from convenient and personalized functions. But convenience should not be obtained by turning consent into a single compulsory button. Where different processing purposes are involved, different choices should be offered. Where information is not necessary for the basic service, refusal should remain possible. Where consent has been given, withdrawal should remain practical.

Bundled consent should therefore be regulated because it changes the meaning of consent. It makes consent look complete while making user choice thin. Personal information protection should not stop at the record of a click. It should ask whether users had a real chance to know, choose, refuse, and change their decision. Only when these conditions are present can consent function as more than a procedural formality in digital services.

References

China Internet Network Information Center. (2026). *The 57th statistical report on China's Internet development*.

Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, & State Administration for Market Regulation. (2019). *Methods for identifying illegal collection and use of personal information by apps*.

Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, & State Administration for Market Regulation. (2021). *Provisions on the scope of necessary personal information for common types of mobile internet applications*.

Ministry of Industry and Information Technology. (2026, March 13). *Notice on apps and SDKs infringing users' rights and interests, 2026 No. 2, total No. 55*.

Standing Committee of the National People's Congress. (2021). *Personal Information Protection Law of the People's Republic of China*.

Supreme People's Court. (2025a, August 28). *Luo v. A Technology Company, dispute over privacy rights and personal information protection, Guiding Case No. 265*.

Supreme People's Court. (2025b, August 28). *Huang Mouhuan v. A Credit Management Company, dispute over personal information protection, Guiding Case No. 266*.