WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 14
LHPPR 2025

Criminalization standard of providing false information in network account transactions and retrieving accounts unilaterally

Wenhao Xia

University of Leeds, Leeds, United Kingdom

Abstract. In online account transactions, the seller providing false information and unilaterally retrieving the account are common actions that may lead to criminal prosecution. However, there is still controversy over the standards for convicting the two crimes in theory and practice. These two behaviours are both standard practices by sellers that harm the interests of buyers, and they may even co-occur in the same transaction. Moreover, under certain circumstances, these two behaviours may produce some ambiguity in definition or interrelatedness, thus making it valuable to study both simultaneously. Regarding providing false information, attention should be paid to its subjective intent and the standards of erroneous understanding. Regarding retrieving an account unilaterally, attention should be paid to its confidentiality requirements and the differences in civil and criminal boundaries and charges involved in the contract. In addition, for the behaviours of both parties, attention should be paid to the responsibilities of the operator platform and the transaction intermediary platform, as well as the establishment of accurate measurement standards for the market transaction value of accounts and the value of user investment.

Keywords: Criminalization standard, online account, false information, retrieving accounts.

1. Introduction

As the global informatization process continues to accelerate, data has become a core element of production and trade. The cross-border flow of data not only promotes the prosperity of the global economy and digital economy, but also provides unprecedented opportunities for countries in scientific and technological innovation and security assurance. Against this backdrop, countries are committed to building efficient systems for cross-border data movement, storage and processing in order to fully unleash the potential of data-intensive technologies and cloud computing solutions.

However, while cross-border data flows create huge economic benefits and promote global collaboration, they also raise serious legal and regulatory challenges. First, there is an obvious mismatch between the rapid development of data flow and the existing regulatory system, and countries face fundamental contradictions in balancing the free flow of data with maintaining national security and protecting citizens' privacy. Secondly, the continued widening of the digital divide has created numerous obstacles for the international community in formulating unified regulatory standards. Countries have adopted diverse and even fragmented regulatory measures out of their own interests. A set of universally binding cross-border data regulatory rules has not yet been formed at the international law level, resulting in a fragmented and lagging global data governance.

In this context, how to build a regulatory framework that can both cope with the rapid development of technology and effectively protect citizens' personal information while ensuring the free flow of data has become a major issue that needs to be addressed urgently. Especially in domestic legal practice, how to effectively connect international regulatory dilemmas with domestic laws and regulations is a major challenge facing legislators and law enforcement agencies. Because of this, the offense of violating the personal information of citizens, as defined by Article 253 of the People's Republic of China's Criminal Code, has emerged as a crucial legal link between the concerns of domestic and foreign data flow oversight.

Therefore, this article will take the crime of infringing on citizens' personal information as the starting point to explore the legal conflicts and law enforcement difficulties that exist in domestic and foreign

regulatory systems in the context of the big data era, and try to provide institutional suggestions for resolving this contradiction.

2. Background of the Study on Criminalizing the Two Behaviors in Online Account Transactions

2.1. Cases of crimes involving online accounts that have emerged in judicial practice

With the further development of the internet and the gradual deepening of the judiciary's understanding of the nature of online accounts, criminal activities involving online accounts are gradually being brought into the judicial perspective. By conducting a full-text search on the Peking University Law Database using an online account as the keyword, there were 439 related criminal cases from 2013 to 2024. It can be seen that a considerable number of cybercrime cases involving accounts have been brought under the jurisdiction of criminal law. Moreover, the basis for trials involving cybercrime is also gradually being improved. As mentioned above, some courts also consider online accounts as private property in their rulings, and the same principle is applied in criminal cases for conviction and sentencing. For example, in the case of Xu Mouliang and Tang Moujie's theft, the two obtained free broadband accounts and sold them for profit. The court deemed this behaviour as theft. Cases involving online account crimes may involve various different behaviours and violate different laws, such as the seller reclaiming the account after the online account transaction is completed, using the pretence of an account transaction to defraud money, or fabricating transaction dispute facts to claim insurance compensation. These may involve fraud, theft, insurance fraud, and illegally obtaining computer information system data (Wang & Zhan, 2023). This article will focus on the seller's provision of false information or unilateral account retrieving actions and their potential involvement in fraud and theft crimes.

2.2. The real-world impact of two types of behaviour

In a judicial environment with a high incidence of fraud, committing fraud through false information in account transactions is common. Relevant studies indicate that in account transactions, fabricating facts related to the transaction leads to the victim misunderstanding the account transaction, thereby deceiving the victim out of their finances. In practice, such behaviour is usually prosecuted as fraud (Wang & Zhan, 2023). Selling a network account and retrieving it through personal information binding is a common form of cyber account crime, and in practice, it is usually recognized as theft (Xu, 2017). For example, in the case where Hu, out of regret, retrieved a game account he had sold, the court found Hu guilty of theft. However, different courts still have disputes over identifying such behaviours in judicial practice. For example, in the cases of Jin Mouqi illegally obtaining computer information system data and Li Hang's fraud case, the defendant's actions both met the criteria for unilaterally retrieving sold accounts. Yet, the courts charged them with illegally obtaining computer information system data and fraud.

Moreover, providing false account information during transactions, which is often prosecuted as fraud, may directly blur the lines or involve complicity with account retrieving. For example, suppose a seller provides false identity information, allowing them to retrieve the account through identity verification after it has been sold. In that case, the distinction between theft and fraud differs from traditional crimes. It can be seen that the boundaries and standards for the criminalization of the two behaviours, as mentioned earlier, still exist in practice, requiring some theoretical exploration for clarification.

2.3. The issues with the current standards for criminalising these two types of behaviour

First of all, unlike traditional financial crimes, financial offences involving online accounts are characterised by their speed and concealment, potentially causing significant financial losses to victims in a short period. Before or during the investigation stage, once such behaviour occurs, it

is difficult to protect the victim's rights. Therefore, how to use judicial intervention to prevent and recover the victim's losses is a problem that needs to be solved.

Secondly, some parties involved in account transactions may belong to different regions, which adds difficulty for judicial authorities in collecting evidence. Therefore, how to take measures to improve the judicial procedures for crimes related to account transactions in order to regulate such behaviours better is also a dilemma in criminalizing these actions.

Finally, the value of an account, as an important criterion for criminalization, still has varying assessment standards. In Li Junyi's article "Criminal Law Protection of Virtual Property," the author categorizes and summarizes the theories of value assessment for virtual property (Li, 2017). Online accounts are a type of virtual property, so this article draws on theories regarding the valuation of virtual property to discuss the value of online accounts. Common models for defining the value of virtual property include the following: the first viewpoint is based on the economic cost and time invested by the user (Liu, 2016). The second viewpoint is to determine based on the official pricing of the online service provider offering virtual items (Zhang, 2006). The third viewpoint is to determine the value of a virtual property based on its market transaction price (Tao & Liu, 2007). The fourth viewpoint is that different types of virtual property should be distinguished. At the same time, various methods of calculation should be adopted for the legal interest entities that own virtual property (Zhang, 2015). It can be seen that the valuation of online accounts is controversial and ambiguous. However, since the crimes involved in the seller providing false information or unilaterally reclaiming the account mainly fall under property crimes, the regulation of these two types of behaviour cannot be separated from the valuation of the involved account. This situation leads to difficulties in criminalising and regulating such behaviours. The subsequent sections of this article will discuss the pros and cons of various valuation methods and solutions to this dilemma in specific situations.

3. Standards for Determining the Criminalization of Two Types of Behaviour

To address the difficulties mentioned above, it is necessary to discuss the details of the criminalization of these two types of online account-related offences. This section will explore the details of the criminalization of these two behaviours separately.

3.1. Discussion on the standards for recognizing fraudulent behaviour by sellers providing false information

3.1.1. The seller's subjective intention in providing false information

Suppose the act of the seller providing false information in an online account transaction is deemed as fraud. In that case, the seller's subjective intention should be described as deliberately transmitting false details on the relevant online account, causing the buyer to misunderstand and thereby illegally obtain the buyer's finances. However, such subjectivity has a certain degree of difficulty in proving. On one hand, online accounts possess the attributes of electronic data, which makes their various features somewhat complex, and there will inevitably be information asymmetry in the communication and coordination between the two parties in a transaction. On the other hand, in this situation, the proof of subjective standards relies on online chat records and conversations, making it difficult to measure the actual degree of subjective malice. If all instances where the buyer receives an online account with inconsistent information before the transaction are hastily deemed fraud, it will lead to an overly dense legal net. It may negatively impact the market for online account transactions. Therefore, determining fraud in such behaviours should be considered in conjunction with the transaction.

First, the criteria for criminalizing this behaviour should require that the seller does not intend to complete the account transaction in a usual market manner. This usual market manner includes the seller selling the corresponding online account and the transaction amount not significantly exceeding the buyer's expectations based on the information provided. Under this standard, transactions

involving accounts that did not exist from the beginning should be deemed to possess the subjective elements of fraud; however, mere errors in understanding some key information about the account are insufficient to prove that the seller possesses the subjective elements of fraud. In the case (2020) Zhe 0110 Criminal First Instance No. 750, in the fraud case involving Huang and others, Huang and others fabricated the security deposit funds and did not have any actual trading accounts. This situation lacks the subjectivity to complete the account transaction under normal market conditions.

Furthermore, after the buyer suffers a loss, the seller's actions influence subjective determination. Suppose the seller immediately takes remedial measures to reduce the buyer's loss after the buyer suffers a loss. In that case, it can be considered that the seller did not have the intent to defraud and should not be deemed as committing fraud. Suppose the seller, after selling the account and causing economic loss to the buyer, takes advantage of the characteristics of online transactions by deleting contact information and transferring the proceeds of the crime to evade investigation and protect the illegally obtained finances. In that case, it can be deemed to have the subjective intent of fraud.

3.1.2. The standard is sufficient to cause the buyer to have an error in perception

For general fraud cases, the standards for causing a sufficient error in perception mainly fall into two categories of theories. One theory leans towards using the standard of the average person in society; if the act is misleading to them, it can be deemed sufficient to cause an error in perception (Zhang, 2005). Another school of thought advocates examining the actual circumstances of the victim to evaluate whether the deceptive act is sufficient to mislead the victim (Li, 2016). In the context of fraud crimes related to online account transactions, considering the actual situation of the victims may be more reasonable. This is because online accounts are a new phenomenon, and various online platforms are iterating extremely fast. Different ages, identities, and professions have varying levels of understanding of different types of online accounts, making it challenging to summarise standards for an average person. Therefore, to better determine the standard for causing a misunderstanding, the judiciary should take into account the specific circumstances of the victim to judge whether the extent of false information in the account in the case is sufficient to cause the victim to have an error in perception.

3.1.3. Determination of the amount of crime

Determining the criminal amount for this behaviour should depend on the amount paid by the victim in the transaction and the value of the account involved in the transaction. In the previous text, four theories for defining virtual property were mentioned. For fraudulent activities in online account transactions, the theory of determining the value based on the market transaction price of the virtual property itself should be adopted (Tao & Liu, 2007), because the value of online accounts, compared to other types of virtual property, is difficult to determine through means other than transactions. This behaviour itself occurs within transactions, using market transaction prices as a standard can more conveniently measure its value. In summary, regarding the act of the seller providing false information in online account transactions, if the online account itself does not exist, the amount paid by the victim shall be considered as the amount of the crime;If the victim obtains the online account, and the value of the online account alone differs significantly from the information provided by the seller, the market value of the online account needs to be assessed, and the difference between this value and the amount paid by the victim should be considered the amount of the crime.

3.1.4. The relevant responsibilities of online platforms

Evidence collection and investigation have specific difficulties, mainly due to the potential distance between the parties involved and the reliance on less stable types of evidence, such as chat records or statements from the parties. Therefore, it is necessary to find a medium that can effectively record the valid transaction information of both parties to assist in the investigation and evidence collection. Account transactions mainly involve two types of platforms: intermediary platforms and account operation platforms. The intermediary platforms primarily handle various matters related to account transactions. In contrast, the account operation platforms manage account real-name verification and

identity information, among other things. If only the victim reports the case and cooperates with the investigation, there are specific difficulties in collecting evidence and tracking the suspect. Suppose we can leverage the information registered on intermediary platforms and account operation platforms. In that case, we can more quickly identify the criminal suspects and prevent further losses to the victims by freezing the involved accounts.

For account transactions conducted through intermediary platforms, clarifying the relevant obligations of these platforms and improving the compliance of their service contracts can ensure that they assist law enforcement agencies in timely reporting, providing evidence, and even coordinating between buyers and sellers to prevent criminal activities. This can positively promote the prevention and investigation of such cases.

Whether or not the account transactions go through an intermediary platform, relevant evidence can be collected using the account's operating platform. Although requiring account operation platforms to monitor the transaction status of the numerous accounts they register is not practically feasible and places an excessive burden on these platforms, it is achievable to authorize them to provide relevant information as evidence when related cases arise. Even though providing such information may risk violating pertinent provisions of the Personal Information Protection Law, it can effectively handle cases with the voluntary consent of the parties involved.

3.2. Discussion on the standards for recognizing theft when the seller unilaterally recovers the account

3.2.1. Define and delineate the seller's unilateral account recovery behaviour

The unilateral account recovery behaviour discussed in this article refers to the act of the person recovering the account through the identity information linked to the account after a typical transaction without the seller's consent. The reason for this behaviour lies in the fact that online accounts have specific personal attributes. As the original account holder, the seller can use their bound identity information to retrieve the sold account through the account operation platform. It should be noted that if the seller retrieves the account due to reasons attributable to the seller, such as the buyer agreeing to return the account, or if the seller retrieves the account due to the buyer's fault, it does not fall within the scope of this action.

3.2.2. The necessity of the secrecy element in the crime of theft in this act

As mentioned above, the academic and judicial circles consider this behaviour to constitute theft (Xu, 2017). Regarding the determination of theft, traditional views hold that it needs to be conducted secretly (Chen, 2003), some new perspectives suggest that the element of secrecy in theft should be downplayed (Zhang, 2006). Regarding the definition of this behaviour, this article believes that the element of confidentiality is necessary. Because such behaviour is based on the use of online accounts, the change of passwords and login alterations of online accounts determine the actual possession changes. This process is extremely short and easily detectable by the original owner. Its lack of secrecy means that the buyer is fully aware of the seller's retrieval actions, which could be considered tacit consent to the retrieval. In this case, it is generally not considered the behaviour discussed in this article and is not deemed a crime.

3.2.3. The civil and criminal boundaries of breaching contractual obligations and the boundaries with contract fraud

From the civil law perspective, this behaviour may be considered a breach of the contractual obligations of the account transaction between the two parties. Nevertheless, this behaviour involves the actor secretly retrieving the sold item after the civil transaction is completed, which meets the elements of the theft crime. Therefore, the criminalisation of this behaviour should focus on the timing of the account retrieval, distinguishing it from the behaviour of automatically terminating a contract in a civil contract.

Furthermore, contract fraud may be suspected due to its high correlation with sales contracts. However, the transactions discussed in this article are conducted legally, so there is no false contract, and the elements of contract fraud are not present.

3.2.4. Discussion on the determination of the amount

The criminal amount of this behaviour depends on the value of the involved account. Regarding the discussion of the criminal amount of this behaviour, this article tends to favour the economic cost and time theory invested by the user (Liu, M. 2016),and determine it based on the value of the virtual property itself, that is, the market transaction price (Tao & Liu, 2007), the two theories are combined for determination. Since the account, in this case, has undergone a complete and legal transaction, it is relatively convenient to include it in consideration of account value; moreover, when the buyer purchases the account, they may also invest specific economic and time resources into the account, thereby altering its actual value. Therefore, this portion of value should also be additionally considered.

3.2.5. Mitigating and lenient circumstances of the perpetrator

Since online accounts fall under the category of electronic data, they are particularly susceptible to tampering. After an online account is recovered, certain actions by the original seller may cause the account's value to depreciate significantly quickly. To prevent this situation, it is significant to reasonably set the mitigating and lenient circumstances for the perpetrator's actions, return the criminal proceeds, and prevent the victim's losses from expanding.

Therefore, to better protect the interests of the buyer as a victim and regarding the relevant mitigating circumstances of fraud and theft, sellers are encouraged to safeguard and return the buyer's rightful account property to promptly compensate for the damage caused to the buyer and prevent further harm. Due to online transactions' fast and efficient nature, the return of online accounts should also not involve overly complicated procedures and costs. After accepting a case, public security and judicial authorities should actively guide the offender to comply with the provisions of the criminal law regarding the return of stolen property and compensation to promote a lighter or reduced sentence, thereby minimising the victim's losses and achieving the goal of compensating the victim. Moreover, in such cases, those who promptly return the account after the case is accepted and do not cause any depreciation in the account's value can be considered not to have committed a crime. This approach better protects the interests of multiple parties involved in the case and saves judicial resources.

4. Conclusion

Regarding the behaviour of the seller providing false information, the determination of the seller's subjective intent should refer to whether the seller has the subjective intent to conduct normal market transactions and the seller's behaviour after the buyer suffers a loss; in such cases, the standard for sufficient misunderstanding should consider the specific circumstances of the victim in judicial proceedings. Regarding the seller's unilateral action to retrieve the account, it should meet the requirement of secrecy; moreover, this action should be distinguished from the default termination of a civil contract, given that the contract itself was legally performed. Such behaviour cannot constitute contract fraud. Regarding the criminalization of such behaviour, reference should be made to the relevant mitigating and lenient circumstances of fraud and theft crimes, encouraging sellers to safeguard and return the buyer's rightful account property better to protect the interests of the buyer as a victim. For these two types of behaviour, the obligations and responsibilities of transaction intermediary platforms and account operation platforms should be clearly defined to assist in the judicial process of related cases and protect the interests of the victims. Regarding determining the crime amount, a measurement system for the market value of account transactions and the value of user investments should be established to determine the criminal boundaries of these two behaviours.

References

[1] Chen, X. 2003. Normative Criminal Law. China University of Political Science and Law Press: 499.

[2] Li, H. 2016. Criminal Law Theory (2nd Ed.). Law Press China: p313.

[3] Li, J. 2017. The Criminal Law Protection of Virtual Property. Journal of Chengdu University of Technology (Social Sciences) 25 (04), 50-56.

[4] Liu, M. 2016. Qualitative Study on the Theft of Virtual Property in Cyberspace. Law science (01), 151-160.

[5] Tao, X & Liu Z. 2007. On the Legal Protection of Virtual Property in the Internet. Political Science and Law (04), 96-100.

[6] Wang, P & Zhan, J. 2023. Judicial Regulations of Property Infringement Acts Involving Online Game Account Transactions. Journal of Criminal Investigation Police University of China (06), 66-77.

[7] Xu, L. 2017. Dogmatic Analyze on the Crime against Virtual Property. The Jurist (04), 44-57+176.

[8] Zhang M. 2005. On the Property Disposition Behavior in Fraud Crimes. China Legal Science (5): 118.

[9] Zhang, M. 2006. The Difference between Theft and Plunder. The Jurist (2): 119-131.

[10] Zhang, M. 2015 the nature of the act of illegally obtaining virtual property. Supreme People's Procuratorate of People's Republic of China.

[11] Zhang, Y. 2006. Discussing the Determination of the Value of Virtual Property in Online Games. People's Judicature (11), 74-75.