

Learning about the Characteristics of the Initiation of Information Crime

Haidar Hassin Ali Kriti^a, ^aFaculty of Law, University of Karbala, Iraq, Email:
^aHaider.hussein@uokerbala.edu.iq

This study premised that the information crime passed through several stages from initiation to execution and commitment of the crime. The crime however may or may not end as desired by the actor as it may suspend at the stage of initiation and fails to achieve its motive. This study seeks to examine whether it is possible to understand the initiation of an information crime especially in the context of criminal jurisprudence. The Law asserts that there are crimes in which initiation is not achieved, such as unintentional crimes where the criminal intent is not envisaged, as well as the crimes of which the material corner is a failure to act. This research was carried out in two parts: first, to know the nature of the information crime, its meaning, its definition and its characteristics; and the second part determined the possibility of initiating the information crime. During the second part, it was necessary to understand the concept of initiation as well as to comprehend the elements of initiating the information crime. The study has useful implications for legislators to take precautionary measures while framing laws related to information crime. The study also framed suggestions and recommendations as to how to prevent information crimes.

Key words: *information crime, initiation, Cybercrime, physical corner, moral corner, characteristics.*

Introduction

Technology in nature is morphing and expanding to such an extent that it might not have only the potential to enhance human lives, but also negatively affect human. The greatest threat that has occurred is perhaps in the field of computers and information networks making both positive and negative effects on human life and behavior (Jessica, et al., 2019). Positive impacts include making the whole world a global village with a robust communication network and the internet. Technical development has helped speed the circulation and ease of information (Roya and Nima, 2019), as well as the diffusion of cultures and facilitation of trade activities



globally. Technology helps in strengthening the human relationships by increasing their connectivity and speedy delivery of messages reducing the paper costs; however, besides this positive usage of technology, there also looms negativity, especially in the use of computers and Information networks for illegal purposes or more precisely for the commission of criminal activities (Mkrtchian, 2019).

Information crimes can be committed in multiple forms, individually or in groups; locally or globally; at a personal or at an institutional level. Researchers and experts in legal studies have not agreed on a particular terminology due to its increase in scope and sophistication. Some of them use the term "informational crime" (Mkrtchian, 2019) while others call it 'cybercrime' (Takashi, et al., 2018) due to the excessive use of computers and the Internet to carry out criminal activities. Some jurisprudence also uses the term 'technological crimes' or 'cybercrime offenses', 'computer abuse crimes', 'High-tech crimes' or 'computer-related crimes' (Tomáš, and Jakub, 2019).

This study is primarily designed to understand the definition and meaning of information crime in the light of criminal offences committed. The focus of the study will however remain on examining the crime in which the actor is unable to achieve his or her criminal outcome, regardless of his or her efforts, for reasons beyond his control. The study will also exclude from its scope and definition actions such as solitary crimes that are committed by single actors or aided by others for achieving their personal vested criminal outcomes or such crimes which are committed for specific purposes and cannot be generalized.

This research will hence use the term 'informational crime' in the light of definitions provided by some researchers (Silva, 2017): it is explained that computer crimes or technological crimes do not always mean crimes committed in the field of computers and information networks through the Internet. In fact, technological crimes may also often include crimes that are not categorized as information crimes. It is basically the computer and information networks that serve the means by which information crimes are committed. Information criminals use computers and information networks to obtain, delete, change, add or destroy information. Such information could be related to people's lives, their private data related to their health, finances, banking, and conversations on social media accounts, browsing history, website passwords and a like. Technology has made human lives digital, and such digital information can be accessible to potential perpetrators, who can be termed as cyber criminals or hackers. The more digitization becomes abundant and ubiquitous, the more information becomes prone to risks and threats.

Due to its complexities of definition and understanding, a need was felt to examine the widespread span of such information crimes in order to enable a universal and standard definition of it. The concept of information crime has undergone a huge development over



time, in both scope and sophistication, owing to the increase in the varieties of means of information technology and information networks. These means have given rise to the development of new techniques and methods in committing crimes; for example, hackers or criminals manipulate data stored in computers and make its use illegal.

Initially, when information crimes began to be committed, the reaction was limited to mere publication of a few newspaper articles to disseminate and educate masses about these illegal acts and discuss how to deal with them. In the mid-1970s and early 1980s, dealing with illegal acts in the cyberspace environment and information networks appeared to be a new criminal phenomenon and not merely immoral behavior (Guimaraes, *et al.*, 2018). Hence, a dire need was felt to address this serious phenomenon, technically and legally. Technically, the security of data was emphasized through the use of passwords, especially to prevent anyone else other than the users from viewing the data; later, the focus moved to protect information from tampering or manipulation (Forsman, and Niklas, 2017). From the legal point of view, the experts in jurisprudence studied this phenomenon of information crime in order to devise effective solutions.

The next section attempts to define information crime as it developed the language that is used to understand and both the narrow and broad implications. This is followed by a methodology to designate a right term for this phenomenon by highlighting the characteristics of the information crime committed with the use of computers and information networks.

Information Crime: Language and Meaning

The term 'crime' originally meant an "offense" or a "sin" committed (Allen, 2015). As for the term "information", it refers to knowing or making a sign about what is known (Tina M., et al., 2016). The term "information" is self-explanatory and was first used by Philippe Dreyfus, who used this term to define the science that links computer science (Stefania, and Michela, 2018). It is however difficult to define exactly what information crime is, but there are experts and jurists that have given relevant definitions. Perhaps one of the most important definitions of information crime is that of al-Faqihan Micel-Credo, who said: Information crime is the "misuse of a computer as a tool to commit a crime amounting to unauthorized access to the victim's computer or data, and such a crime also includes physical attacks on the computer itself or its related equipment (Kyle, and Michae, 2013). It is also known as "a crime carried out in the periphery of a computer (Chishti, and Mahreen, 2019). According to these definitions the mere commitment of criminal behavior in the vicinity leading to a disruptive act amounts to information crime.

Hence, scholars have differed in defining "information crime" and as it dealt with many doctrines and concepts. There is no doubt that reasons for such difference in opinion and understanding of the information crime are many, the most important of which is a continuous



novelty and sophistication in this crime; the differences of views of the experts in its study; and, the frequent variation of methods in which this crime is committed. In any case, it is necessary to clarify before the delineation of information crime that the scope of the crime is not acts or omissions that constitute an attack on a computer or any of its material components, such as theft, corruption or otherwise, (Nye, Robert A., 2014); but it constitutes the unlawful assault on computer data, intended to mean negative acts that are committed within the scope of information.

Additionally, it is also not acceptable to describe any crime as the information crime in which a computer or any of its components or material components are assaulted. There is a difference between crime committed to some information in the form of infringement, breach, or stealing the data and the crime in which an information system is used as a tool of crime. Hence, one cannot call the latter case information crime, but rather an ordinary crime, where physical components of an information system are abused or attacked. Hence crimes committed on computers or on printers and other devices are ordinary crimes, but on the other hand, a person who uses the information system to intimidate another person or enter into a company's server with a view to destroy, alter, or manipulate the information contained within the network of its computers is considered to be information crime (Wazoel, and Philip, 2017).

This leads to conclude that, the intent of the information crime is significant and for any such illegal act the knowledge of information technology is fundamental (Ronald F., and Aric, 2018). According to this definition, knowledge of information technology is required to commit any informational crime, and that those conducting investigation and prosecution must have technical knowledge. This definition also restricts the concept of information crime and is not applicable on cases where a little or only basic knowledge of information technology is required. However, such a condition is not significant because an information criminal may not possess a large amount of knowledge and skill in information technology when committing an information crime. In fact, there exists the inertia for the user inside the computer itself that provokes him to commit an information crime when there is an opportunity. Hence, in order to evolve into an information crime, it does not require a large amount of experience in the field of computers.

One of the narrow-term definitions of cybercrime relates it to a crime against money associated with automated information processing (Sabah, et al., 2019) or "any negative or positive conduct under which programs or information are attacked in order to take advantage of any image" and that "any act or omission that attacks moral funds (computer data) and that is a direct and indirect result of the intervention of technology. Information can also be defined as any act of "positive or passive intentional to attack the technology of information" or an act carried out by complex electronic devices in order to cause harm (Sabah, et al., 2019; Hashim, et al., 2019).



Some jurists have however differed in the definition of information crime and recommend to set objective and standard criteria to understand it (Jurdi, 2017). These jurists insist that the definition must contain all the elements of crime and its impact and must be stable and consistent among all juristic situations, including physical as well as moral pillars of jurisprudence (Claus, 2006). Legally, in the field of jurisprudence, when an information crime is committed there is a provision of the punishment or measure imposed by the law. Therefore, in the field of jurisprudence, the definition of information crime will be: Any positive or negative act of which the information system is a tool or a means to execute and that it constitutes an attack on a law-protected interest or an act that the law punishes as a penalty (Marianthi, et al., 2005).

The examination of the above-mentioned definitions of information crime leads to an understanding that these definitions are more universal than consistent. It is also observed that these definitions restrict the assault on money; they are regardless of material or moral consequences; they require that the criminal act be intentional or causing harm to others. One thing that is common in all definitions is that the culprit may use the computer and communication networks to attack people's lives or to violate the sanctity of their personal lives (Diss. 2016). The information crime is also not required to be deliberate as it may be unintentional. If the criminal intent of the offender is neglected, he might direct his will to the correct destination. For example, a person may delete information from the computer's memory of a person by negligence or error, which may not amount to an information crime.

Information Crime: Language and Characteristics

In this subsection, the characteristics of information crime have been identified. The crime of information is only the result of technological or scientific development in the field of computer and information networks, so it is this development that gave this crime some characteristics or enhancement of the purpose of this kind of crime. Such characteristics may also be associated with a cybercrime relationship with computer and information technology. The more widespread this technique, the more this type of crime is committed.

In order to understand the characteristics of information crime, it is required to first identify instruments or methodology used to commit the information crime and then look for evidences and discovery of the crime. The methods by which a criminal offence is committed is generally defined as: a tool or a machine that intervenes or mediates between the criminal will and the crime; in other words, a criminal method is the means by which the perpetrator may resort to and use to achieve his criminal will (Jurdi, 2017). This makes information crime having a distinct characteristic from other crimes because the method of committing information crime is often solely through a computer.



However, in jurisprudence, making the computer the only means to commit the crime of information may be treated as a limited definition (Wazoel, and Philip, 2017). The information crimes may also be committed through electronic devices other than a computer, such as a mobile phone or an electronic tablet. Such devices like a mobile phone or a tablet can participate in information networks, whether local or international, through the Internet and implement the crime. The Law believes that this is an era of information revolution, and therefore it is possible for science to invent new electronic devices that could be used as a tool to commit information crime (Tina M., et al., 2016).

The commitment of information crime also requires technical knowledge in the field of computer and information networks. In the recent past, information crimes were committed by people with experience and expertise in computer technology and information networks. A computer program is written in special languages that require knowledge of procedures, and programming credentials. A computer programmer, having the knowledge of Fortran or Linux languages will take only a few hours to commit a crime. This is one of the reasons that people with a good technical knowledge are often engrossed in cybercrimes.

Another characteristic feature of information crime is the difficulty of finding evidence in order to prove that a crime has been committed specifically. It is also difficult to prove the motive behind this kind of crime as this crime differs from other crimes in terms of material evidence left by the offender at the crime scene. There are many evidences in other types of crimes by which the truth of crime can be reached. For example, in murder crimes, a criminal leaves traces of blood or the body of a victim or there is a broken door as the evidence of a crime of theft. However, in information crime, the perpetrator can, in a few seconds, erase and destroy all evidences of his crime. The information crime is also often committed by manipulating information, which is also another reason for not being able to detect the information crime. More importantly, if it is hacked from outside the borders, there is no material proof of such an intangible act. In all such cases, computer officials do not report violations committed, in order to avoid problems of being charged for negligence or failure of security measures.

The difficulty of finding or proving the information crime can be due to many reasons namely: First, there is often no evidence of the crime, in which the responsible person could be found guilty (Kristen D., and David, 1979). Second, the perpetrator of the information crime has the expertise and skill to hide the evidence in order to avoid being condemned. Third, there is a lack of experienced investigative or judicial authorities in the field of computers and information networks. These crimes often require investigators with technical expertise. Fourth, mostly such information crime are not reported because the victim is often a large financial institution or a large commercial or industrial company and refrain from informing the competent authorities about the occurrence of information crimes and maintain confidence of customers. Such institutions also fear that the financial reputation of these institutions or



companies can be at risk if such crimes are made public (Kristen D., and David,1979). Lastly, it is also difficult to track the perpetrator of the cybercrime in any given network due to its large scope and sophistication.

Initiation of Information Crime

The next question in the current study is to find out whether it is possible to initiate the information crime. In particular, though, there are crimes that cannot be initiated, either wholly or completely, such as non-committal crimes and crimes whose physical element is to refrain from doing (crimes of negation). However, an attempt can be made to understand how this information crime started and what various starting points were. It is important to first define initiation and then look into its various types.

A number of writers have introduced initiation, some of whom have defined it as "an incomplete crime" or a crime in which "the physical element is not fully realized" (Takashi, et al., 2018). In the domain of criminal laws, a definition can be cited given by the Iraqi Penal Code No. 111 of the year 1969, article 30 that it is an " attempt to begin to carry out an act with the intention of committing a crime or misdemeanor unless it is stopped or is disappointed by the consequences."

The Jordanian Penal Code of the year 1960 in the article 68 defined initiation as an act of manifest that leads to the commitment of a felony or misdemeanor. If the perpetrator is unable to complete acts necessary to obtain such a felony or misdemeanor, he shall be punished in the stipulated manner unless otherwise provided by law such as hard labor, permanent or temporary in a termed imprisonment for seven to twenty years. The penalty of felony can also be imposed for at least five years with hard labor, or life imprisonment.

Article 30 Of the Iraqi Penal Code postulates that initiation can be of three types with the common denominator between these three types being the non-achievement of results of the criminal intent of the object which may be because of the lack of physical element or evidence. The three types are first, Getting Started but remain incomplete or crime suspended. This kind of initiation begins when the actor committing a criminal activity (verb) is stopped by reasons or circumstances external to his reach and cannot commit the crime. However, the question that can be raised here is whether it is possible to call an incomplete initiation as the information crime. The answer is yes because if a perpetrator is trying to destroy a program or information through a virus and is interrupted by another person and the virus is deactivated by a counter program. The perpetrator here may be punished for attempting to commit a crime of destroying a program or a computer network.



The second type of initiation is a complete Initiation or Misdemeanor. This happens when the perpetrator commits criminal behavior or an unlawful activity fully and completely. The material element or the motive of the information crime is achieved except that the criminal result of the crime could not be achieved as it was beyond the will of the actor. Here, the difference between the complete initiation and the incomplete start can be observed. Here the criminal behavior is complete in contrast to the former scenario. An example of this type can be cited if a person puts a virus into a computer or a computer network but does not achieve the result that he wanted to because of an antivirus program already installed inside the computer or the information network that prevents the loss of the information data.

The third type is characterized as a crime impossible to commit. The Article 30 of the Iraqi criminal law cited this third type of initiation as a crime committed with the intention of doing a misdemeanor or criminal offense which is impossible to carry out for any reason related to the crime or the means used to commit it shall be considered as a crime. an example can be given if a perpetrator realizes that there is no other way possible to commit a crime just because of the immunity already inbuilt in the act of crime itself.

There is yet another way to look at the information crime which is through the pillars of crime. Generally, there are the two physical pillars and one moral. The first physical aspect of crime is the material activity that the offender commits, taking an external appearance in the form of an attack over an interest protected by the law (Taulan, et al., 2016). The second physical; element is the initiation of the execution of the act of crime as an external activity. Since these are physical acts, therefore it is difficult to talk about their stages of thought, determination, design and preparations for the crime because the law will not penalize for various stages of crime but will punish for the commencement of execution (Taulan, et al., 2016) .With regard to the information crime, this law is also implemented and specifically the Iraqi criminal law would punish any person who initiates an act to commit an information crime.

On the moral perspective, Article 30 of the Iraqi penal code recognizes the existence of moral element in the attempt to commit a crime or misdemeanor. Therefore, the perpetrator must be intended to commit the crime when he commits the act (Takashi, et al., 2018; Taulan, et al., 2016). For instance, a perpetrator may enter an information network in an illegal manner with the intention to commit an information crime and attempts to develop a virus inside the information network in order to destroy or damage it. However, if this is not intended, the initiation will cease, but he can be penalized for the act of entering the information network without permission. It is worth mentioning that the initiation is also applicable to crimes and misdemeanors even without infractions (Taulan, et al.2016).

Moreover, if the perpetrator initiates the suspension of implementation or the manages the disappearance of the impact of both the physical and moral elements, the crime will still be

said to have committed as intended by the offender for reasons beyond his control (Takashi, et al., 2018). The reason is that the crime is not complete for two reasons: either because of the suspension of implementation or the failure to affect the will of the actor. Whatever the reasons, it is a fact that the consequences of the crime were beyond the will of the actor as well its suspension of implementation or the impact of the effect of the act too were not in the will of the actor and therefore the crime could not be committed. It should be noted that the law of moderation, which is not punishable by the legislator, is optional. The actor refrains from completing the crime after it has begun and does not explain the reasons such as fear, remorse or others that led him to refrain from completing the crime.

Conclusion

The advancement in information technology and information networks, particularly due to the Internet usage, has resulted in the most important creations that science could ever offer to humanity or the human mind could invent. However, there is a deviant group that abuses this wonderful technology for criminal purposes. This research study attempted to find out what information crime is and the extent to which this type of crime can cause harm. This study looked at definitions that contained all elements of crime and its impact, in the light of jurisprudence, morality and also the use of Internet as a daily activity medium. The various definitions led to conclude that information crime is actually an act in which the information system is a tool or a means to execute the crime and that it is an attack on a law-protected interest, and that the law shall prescribe a penalty or a remedy to such acts of crime. This study also found out that the offense in the information crime is not restricted to money, whether material or moral, but it could be the attack on the data or the information. Hence, the characteristics of information crime were revealed in the study. These characteristics distinguished information crime from other common and political crimes.

Suggestions and Recommendations

In light of the current study on the substantive provisions for initiation of information crime, the following suggestions can be made. First, it is necessary to update the current Iraqi Penal Code or to enact special penal legislation to accommodate information crime. While doing so, it must be noted what the motives of the initiation of crime were, or whether the law provides appropriate criminal protection for the information system and to its users and whether the user is a natural person or a moral person. It is also necessary that, while dealing with the information crime, the possibility of having it committed cannot be excluded because then it would leave a vacuum which the criminal might use to commit the crime. It is also suggested that specialized institutions and experts in information technology should be employed to determine the identity of perpetrators of information crimes and to understand the nature of their activities and to provide advisory assistance to criminal justice



agencies in tracking perpetrators and determining appropriate sanctions against them. A legal and judicial environment capable of dealing with information crime activities may also be created efficiently and effectively, based on familiarity with the technical and legal aspects of such activities. The experts may also adopt a comprehensive strategy to fight against information crime in which the main sectors of the state should be involved. The government should undertake to study the factors of committing this type of crime, to identify its effects and seek the best means and mechanisms to limit it. Last, but not the least, it is necessary to educate the users about the preventive measures that can be adopted to stop information criminals as well as devise new ways to deal with their behavior in the event of committing crimes.



REFERENCES

- Allen, Christopher W. *Strange Déjà Vu: Tackling Information Sharing Problems for Efforts against Transnational Organized Crime*. Air University Maxwell Air Force Base United States, 2015.
- Balloun, Kristen D., and David S. Holmes. "Effects of repeated examinations on the ability to detect guilt with a polygraphic examination: A laboratory experiment with a real crime." *Journal of Applied Psychology* 64.3 (1979): 316.
- Baur, Elena, Mats Forsman, and Niklas Långström. "Response to Joyal's (2016) 'Linking Crime to Paraphilia: Be Careful with Label'." *Archives of sexual behavior* 46.4 (2017): 867-868.
- Becker, Ronald F., and Aric W. Dutelle. *Criminal investigation*. Jones & Bartlett Learning, 2018.
- Boziev, Taulan, et al. "Computer Tools Increasing the Quality of the Evidence Information Received During the Investigation of Road-Transport Crimes." *Conference on Creativity in Intelligent Technologies and Data Science*. Springer, Cham, 2019.
- de Farias, Adriana M. Guimaraes, et al. "Definition of Strategies for Crime Prevention and Combat Using Fuzzy Clustering and Formal Concept Analysis." *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 26.03 (2018): 429-452.
- Dehgani, Roya, and Nima Jafari Navimipour. "The impact of information technology and communication systems on the agility of supply chain management systems." *Kybernetes* (2019).
- Fantinelli, Stefania, and Michela Cortini. "Informational power and perceived collective benefit affecting the users' preference for a mobile technology: Evidences from a survey study." *Frontiers in psychology* 9 (2018).
- Francis, Jessica, et al. "Does ICT Use matter? How information and communication technology use affects perceived mattering among a predominantly female sample of older adults residing in retirement communities." *Information, Communication & Society* 22.9 (2019): 1281-1294.
- Grivna, Tomáš, and Jakub Drápal. "Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic." *Digital Investigation* 28 (2019): 1-13.



- Hatashima, Takashi, et al. "Evaluation of the Effectiveness of Risk Assessment and Security Fatigue Visualization Model for Internal E-Crime." *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 2. IEEE, 2018.
- Hatashima, Takashi, et al. "Evaluation of the Effectiveness of Risk Assessment and Security Fatigue Visualization Model for Internal E-Crime." *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 2. IEEE, 2018.
- Johnson, Kyle, and Michael Jonsson. "Colombia: Ending the Forever War?." *Survival* 55.1 (2013): 67-86.
- Jurdi, Nidal Nabil. "The Complementarity Regime of the International Criminal Court in Practice: Is it Truly Serving the Purpose? Some Lessons from Libya." *Leiden Journal of International Law* 30.1 (2017): 199-220.
- Khan, Neelam Saleem, Mohammad Ahsan Chishti, and Mahreen Saleem. "Identifying Various Risks in Cyber-Security and Providing a Mind-Map of Network Security Issues to Mitigate Cyber-Crimes." *Proceedings of 2nd International Conference on Communication, Computing and Networking*. Springer, Singapore, 2019.
- Kreß, Claus. "The crime of genocide under international law." *International Criminal Law Review* 6.4 (2006): 461-502.
- Lubua, Edison Wazoel, and Philip D. Pretorius. "Cyber-security Policy Framework and Procedural Compliance in Public Organisations."
- Mahdi, Mohammed Hashim, et al. "Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption." *IOP Conference Series: Materials Science and Engineering*. Vol. 518. No. 5. IOP Publishing, 2019.
- Mkrtchian, Sona M. "Criminal and Legal Protection of Relationships in the Area of Blockchains Functioning and Cryptocurrency Turnover: New Challenges." *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*. Springer, Cham, 2019. 355-361.
- Nye, Robert A. *Crime, madness and politics in modern France: the medical concept of national decline*. Vol. 763. Princeton University Press, 2014.
- Seidu, Hd. *An Examination Of Chieftaincy Institution: The Role And Challenges Of Chiefs In The Socio-Economic Development Of The Dorimon Traditional Area Of The Upper West Region Of Ghana*. Diss. 2016.



- Silva, Francisco. *If we Confess our Sins Abstract I consider the problem a social planner faces in constructing a criminal justice system which addresses two needs: to protect the innocent and to punish the guilty. I characterize the socially optimal criminal justice system under various assumptions with respect to the planner's ability to commit. In the optimal system, before a criminal investigation is initiated, all members of the community are given the opportunity to confess to having committed the crime in exchange* No. 500. 2017.
- Taha, Mustafa Sabah, et al. "Combination of Steganography and Cryptography: A short Survey." *IOP Conference Series: Materials Science and Engineering*. Vol. 518. No. 5. IOP Publishing, 2019.
- Theoharidou, Marianthi, et al. "The insider threat to information systems and the effectiveness of ISO17799." *Computers & Security* 24.6 (2005): 472-484.
- Urban, Vyacheslav, et al. "Implementation of the Law Enforcement Function of the State in the Field of Countering Crimes Committed Using the Internet." *Big Data-driven World: Legislation Issues and Control Technologies*. Springer, Cham, 2019. 113-120.
- Zottoli, Tina M., et al. "Plea discounts, time pressures, and false-guilty pleas in youth and adults who pleaded guilty to felonies in New York City." *Psychology, Public Policy, and Law* 22.3 (2016): 250.