A Review of *Virtually Criminal: Crime, Deviance and Regulation Online*

By

Sz-De Yu
Indiana University of Pennsylvania

Book: *Virtually Criminal: Crime, Deviance and Regulation Online*
Author: Matthew Williams
Publisher: Routledge
Year: 2006

Debates regarding whether the term, community, can be applied in cyberspace have been persisting for a while. The author, Matthew Williams, takes the stance arguing despite the lack of physicality, communities can be formed and maintained in cyberspace. *Virtually Criminal* is centered on a qualitative study conducted in an online community—Cyberworlds. Cyberworlds is an online forum utilizing advanced technology to allow members to present their online persona in a graphic form (i.e. avatar) and to provide interactions other than simply textual communications. Williams uses this virtually realistic setting to examine online deviance and regulations that aim to punish the perpetrators. His theoretical framework incorporates Hirschi's social bonding theory, self-control theory and Sykes and Matza's techniques of neutralization. The essential theme states online deviance stems from weak social bonds to the online community.

The author contends that members who are more socially immersed in Cyberworlds tend to develop stronger friendships, which leads to involvement in conventional activity, commitment to building a positive reputation, attachment to peers and institutions, and belief in the validity of community rules. On the other hand, visitors who view Cyberworlds as a playful site tend to utilize the techniques of neutralization to rationalize their deviant acts. The deviant acts commonly found in Cyberworlds include profanity, harassment, vandalism, and obscenity. Perpetrators are less committed to maintaining their online reputation and less attached to the online community. Hence, they are less likely to be involved in conventional activity and less likely to believe and follow community rules. Moreover, anonymity and the liminal aspect of Cyberworlds help foster antisocial behavior. The liminal aspect, in the author's term, is a quality that contributes to disinhibition in the online community. In short, people who are subject to weak social bonds and whose self-control is reduced by liminality and anonymity are more likely to commit deviant acts in Cyberworlds. Nevertheless, these people also are unlikely to commit more serious acts, for the weak bonds do not allow them to be familiarized with the environment and potential victims, which in turn confines the scale of their deviance.

This study basically focuses on deviance that takes place in the community (i.e. Cyberworlds). Hence, most abuse is addressed to the online persona acting in Cyberworlds, rather than directly to the person who creates it. To consider the harm done,

there is a need to connect the victimized online persona and the creator. The harm mostly stems from text. The brunt of using illocutionary text can harm individuals in a derisory context. Even if the individual does not care much, the harm can be viewed as against the community as a whole. It may still warrant punishment. In terms of punishment, it will likewise be necessary to link the online perpetrator to its creator. The author acknowledges the difficulty in preventing offenders from reentering the community with a new avatar. He also discusses how to employ shaming as a form of punishment. Shaming as an informal social control in tandem with Peacekeepers (i.e. characters in Cyberworlds created and trained to formally enforce regulation) is the mechanism of order maintenance in Cyberworlds, although there are diverse views on their effectiveness.

Order maintenance differs from law enforcement in that violating regulations in Cyberworlds does not automatically implicate a cyber crime, although more and more online deviant acts have been outlawed. There is a concern with the norms and values these regulations are intended to reflect. Williams notes if Peacekeepers are designed to enforce rules merely based on American values, the regulation itself can be biased and not all community members will subscribe to it. In this regard, Williams's study proposes two major findings. First, heterogeneous regulatory approaches are more successful at reducing deviance and maintaining victim satisfaction in Cyberworlds. Second, technology is an effective regulator in Cyberworlds.

This study takes the Internet as a milieu of social and cultural production. Williams adeptly blends sociology, criminology, and linguistics into the explanation of online deviance. As suggested in the book's preface, this book will appeal to students and researchers who are interested in the study of cybercrime, for it presents an in-depth examination of how and why deviance manifests within a community-like setting in cyberspace.

By choosing one particular online forum, Cyberworlds, the study was able to address specific aspects of an online community, which avoids ambiguity that often haunts online research due to the lack of consensual definitions. Thus, constructs, such as anonymity, attachment, and commitment, all have clear operationalization even though this is a qualitative study. In addition, the author cites numerous narratives derived from participants in a focus group. This makes the study more objective, because the reader can see not only the author's interpretation, but also the actual accounts from the members of Cyberworlds.

Aside from these methodological merits, the author demonstrates a good illustration of theory application. The four crucial elements (i.e. attachment, involvement, commitment, belief) in the social bonding theory are adequately addressed. The interaction between online features (i.e. liminality and anonymity) and social bonds is considered and well explained. Complemented by self-control theory and techniques of neutralization, the theoretical framework on which this book is based is solid. This is particularly helpful for scholars who are trying to theorize about cybercrime. This book shows when applying a theory, the social background factors need attention. Therefore,

deep involvement in Cyberworlds can strengthen bonding but also is a requisite for more serious forms of deviance which requires acquaintance with the online community. Moreover, as the author asserts, anonymity although fosters deviance can also enhance social immersion because it actually expedites social interactions in cyberspace, which is contributive to strong bonding.

As much as the author has done an excellent job in terms of research and theory, this book is limited in scope. It is undeniable that Cyberworlds is a special case in cyberspace. Although there are quite a few similar online communities on the Internet, most concerns regarding cybercrime are not really with respect to these community-like settings where a person's online persona serves as the subject in the interactions. Modern cyber threats are more likely to have something to do with people's real identity and usually incur losses in the offline life. For example, identity theft definitely targets real identities. Online sex predators may use online persona to deceive victims but eventually the purpose is to locate the victim's physical presence. Hackers may gain unauthorized access to someone's email account and can result in substantial disturbance in the victim's real life by altering mail content or sending bulk emails. In the examples above, a community-like setting is not required. There will be less collective efficacy as we can find in an online community like Cyberworlds. Hence, what makes sense in Cyberworlds may not be as sensible in the broad cyberworld. Without an avatar, the derisory messages are no longer about my online persona, but rather they are directly about me as a real person. The vandalism will not be on my virtual artifacts which I build in the online community. It may be on my personal webpage or on my computer directly. When the community-like setting is absent, we can still argue there is an online community, only this community can be too big and complex for social bonding to sufficiently explain deviance. In the last chapter of the book, the author tries to expand the theoretical scope to a wider online community, but it seems to fall short. How do we explain college students' prevalent engagement in software piracy? How do we explain those online clubs that pedophiles form? Of course there is some explanation, but it will be beyond the scope of this book. Nevertheless, most cyber deviance takes place in this big community rather than communities as Cyberworlds.

Another salient limitation about Williams' book is that he practically confines his discussion regarding online regulation in a non-legal aspect. Although Williams recognizes the fact that those deviant acts identified in Cyberworlds can be criminal, he seems to be reluctant to include law enforcement in his discussion. The regulation talked about in the book is mainly concerned with what happens within Cyberworlds. Offenders may be shamed, ostracized, banned, or have their accounts revoked, but very little, if any, mentioning about them being held accountable legally. It seems only when online deviance evolves into physical attacks will these deviant acts be considered criminal. However, many cyber crimes do not involve physical contact, such as cyberstalking, hacking, or even virtual rape as mentioned in the book. Neglecting legal issues in regulation does not contribute much to the regulation of online deviance in a broader sense. To be fair, though, the title of this book indeed implies actual criminals will not be the focal concern of this book.

One more thing expected but missing in this book is motivation. Since Williams intends to apply control theory, it is understandable he would exclude factors that are rooted in other criminological theories. Nonetheless, his application of control theory does not elucidate motivation for online deviance. Control theory upholds the assumption that humans were born to pursue self-interests and by pursuing self-interests, it is a natural tendency to become deviant. Therefore deviance needs to be controlled, not to be formed. In this sense, motivation requires no explanation, for it is human nature. However, in Williams's illustration of online deviance, he does not establish why committing deviant acts in Cyberworlds can bring about self-interests for the offenders. More precisely, he fails to define self-interests in cyberspace, or particularly in the community of Cyberworlds. It would be somewhat questionable if we assume they represent the same thing both online and offline, since it is acknowledged interactions online are reinforced and facilitated differently than those offline. On the Internet, many youngsters will be ecstatic if they have a lot of visiting to their personal webpage everyday, but they may not like a crowd visiting their home everyday. It is suspected that gratifications resulting from online activity can be slightly or vastly different from gratifications resulting from offline activity. After all, vandalizing a house by painting is not quite the same as vandalizing a website by hacking.

The critique presented in this review is not to discredit Williams's study or book. As a matter of fact, *Virtually Criminal* is a good source of knowledge. First of all, it provides detailed examination in the interaction modes on the Internet. The interaction can be only-text or can be graphic or can be in the form of artifacts, such as websites. Different social settings will influence interactions in different ways. Second of all, this book offers an opportunity for readers to see how interdisciplinary theories can be integrated. Furthermore, the author spends some space addressing online deviance and its effects from a linguistic angle, which is a rare aspect for most criminologists. Despite the limitations on its generalizability, overall this book is especially recommended to students who want to take a deeper look into social structure and processing in cyberspace, and also to researchers who desire to conduct qualitative research on cybercrime, communication, and community interactions in cyberspace.