SENTENCING POLICY AND PROCEDURE AS APPLIED TO CYBER CRIMES: A CALL FOR RECONSIDERATION AND DIALOGUE

Donald R. Mason*

I am very pleased that we have devoted the concluding half day of this conference to topics relating to the intersection of sentencing and Internet victimization.¹ This is of very special interest to me because I teach courses in both cyber crime and sentencing here at the University of Mississippi School of Law.

I. SENTENCING REGIMES AFTER BOOKER

Within the last three years, the United States Supreme Court has dramatically shifted the landscape of sentencing law. In Blakely v. Washington,² the U.S. Supreme Court ruled the State of Washington’s sentencing guidelines were unconstitutional because they allowed a judge to enhance criminal sentences based on facts not determined by a jury or admitted by a defendant. Constitutionality of the Federal Guidelines,

---

¹ Associate Director of the National Center for Justice and the Rule of Law at the University of Mississippi School of Law. Prior to joining the NCJRL, Mason served as Senior Legal Research and Training Attorney for the National White Collar Crime Center, developing and presenting legal training on computer crime, computer related criminal investigations, and other white collar crime topics. Mason began his legal career as a prosecuting attorney in his native state of Iowa. He then served for twelve years as the Iowa Prosecuting Attorneys Training Coordinator and Executive Director of the Iowa County Attorneys Association, coordinating statewide training, technical assistance, and governmental liaison.

similar to Washington's, were called into question. In United States v. Booker, the Court extended the Blakely rationale to the Federal Sentencing Guidelines and rendered those guidelines advisory. Although Booker concerns the right to a trial by jury, the decision has significant ramifications for the policy and law of sentencing.

Although this training conference is intended for state prosecutors, a review of the changes in the law and policy behind the Federal Sentencing Guidelines is relevant for several reasons. First, the Federal Guidelines, rightly or wrongly, are the “800-pound gorilla” in the room. The federal government prosecutes more crimes than any individual state in the area of cyber crime, and thus generates the most case law and commentary on the nexus between cyber crime and sentencing policy. Second, because many states have sentencing schemes similar to the ones invalidated in Blakely and Booker, federal precedent affects approximately one third of all states directly. Booker also affects all states indirectly to the extent the Supreme Court addressed constitutional issues in sentencing. Third, the rationales expressed in federal cases, particularly landmark cases such as Booker, are highly persuasive to legislators and other policymakers. For example, Booker emphasized that sentences must be “reasonable,” rejecting the idea that a statute, no matter how well crafted, can replace the well-informed discretion of a sentencing judge. In this respect, Booker can be seen as a continuation of the sentencing reforms of recent decades.

With an increased focus on the policy of sentencing, a review of the traditional theories of sentencing is in order. Sentencing has traditionally been defined by two inputs: the seriousness of the offense and the characteristics of the offender. The seriousness of the offense is both qualitative (typically a requisite mental state) and quantitative (financial loss, number of victims, and other factors). The key question asked

\footnote{United States v. Booker, 543 U.S. 220 (2005).}

\footnote{Id. at 262-64.}
in this line of thinking is how we measure the harm caused by the illegal act.

The second input is the characteristics of the offender: his or her criminal record, culpability, willingness to accept responsibility (by plea bargain or during the sentencing phase), and so forth. The key question asked in this line of thinking is whether the defendant's conduct aggravated the offense or mitigated it. Rationales of punishment include deterrence, incapacitation, rehabilitation, retribution, "just deserts," and restorative justice.

II. HOW CYBER CRIMES ARE DIFFERENT

When addressing the nexus between sentencing and cyber crime, a fundamental question is: what is cyber crime? Most conferences on cyber crime focus on the offenders: who commits these kinds of crimes and how they commit them. Moreover, most training is devoted to how to detect cyber crime, apprehend the cyber criminals, and then prosecute them. Very little attention has been given to post-conviction matters, such as sentencing, victim impact, or alternative resolution. In preparing for the conference, it was very difficult to find people who were experts in both sentencing and cyber crime. I believe this touches upon an important shortcoming in our cyber crime jurisprudence: we have not yet adequately considered whether the traditional models of sentencing "fit" with cyber crime.

Cyber crime is both similar to and different from traditional crime. In many respects, traditional crimes have simply taken different forms by "migrating" to the Internet. For example, an e-mail fraud is quite similar to a traditional fraud. Scholars have debated whether cyber crimes are truly new and different crimes or just "old wine in new bottles." Certainly, from the perspective of law enforcement, the crimes are often very similar—we apprehend the criminals, analyze the

---

evidence forensically, and present that evidence at trial much the same way regardless of the type of crime. The tools and techniques for commission, detection, apprehension, evidence analysis, and presentation methods have all adapted to the evolution of technology and the Information Age.

However, cyber crime is also different in many ways. It is often very difficult to detect, which presents new challenges for prosecution. It can also involve more complex potential for secondary and continuing victimization, even after perpetrators may be behind bars, such as when images of child pornography are distributed long after the abuse, or when a virus continues to replicate or is altered and re-released. Cyber crime is also less often a crime of passion, rage, or economic desperation, and more often a crime of defiance, overcoming a challenge, technological opportunism, or simple curiosity. The psychological motivations of cyber offenders are substantially different from those of traditional criminals. One scholar has also recently suggested that generativity is a key difference between cyber crime and traditional crime.\(^6\)

During the first two days of this conference, a number of thought-provoking comments led me to think that perhaps it is in the aspect of victimization where cyber crime is most distinguishable from traditional crime. Cyber crimes can have a much more widespread impact upon a much larger number of victims per offense. They also present new and difficult issues regarding vulnerability of Internet users. Furthermore, prosecution of these crimes is more problematic because of the practical challenges of securing victims who can be available to testify, as well as the jurisdictional issues presented by interstate and international conduct. Finally, cyber crime often lacks a clearly identifiable victim, or worse, involves conduct from which victims are unable, in contrast to “traditional” crimes, to confront or “put a face on” the perpetrators. Law enforcement has traditionally been able to put a face on specif-

---

ic victims and perpetrators of criminal acts, but this is frequently not true with Internet crimes.

III. SHOULD SENTENCING LAW AND POLICY TAKE INTO ACCOUNT THE DIFFERENCES BETWEEN TRADITIONAL CRIMES AND CYBER CRIMES?

These considerations cause me to ask: can or should our old rules and policies regarding sentencing and punishment apply? When we talk about investigating cyber crime, we frequently assert that constitutional rules of criminal procedure pertaining to traditional crime apply in the same manner to cyber crime, only with some nuances. But what about our sentencing purposes and procedures and our societal purposes of punishment? Those fundamental concepts for responding to criminal conduct may well be radically different with regard to cyber crime. For example, if a cyber criminal is not motivated by forces the same as or similar to those motivating a regular criminal, our traditional models aimed at deterrence might not work well, or not work at all. Likewise, when the fact or scope of Internet victimization is undiscovered or difficult to detect until long after the event, our traditional models of measuring harm might fail to adequately address the problem.

In the courses I teach on sentencing, most of the material and discussion focuses on traditional crimes. When we consider the so-called “traveler” cases involving attempted sexual exploitation of children and the varieties of Internet fraud, for example, I have to wonder to what extent we are hitting the mark with sentencing. Does the digital and Internet age challenge or require us to re-examine our notions of case disposition and punishment? What should we do differently? If our goals may be different with regard to cyber criminals, what should our primary sentencing goals be? Do we seek to impose punishment that approximately equals the harm done, or do we focus on deterrence? Do we seek to rehabilitate offenders, or should we focus on protecting the public through incapacitation? Should our sentencing practices and concerns focus more on the offender or on the harm caused to victims?
On the concluding day of the conference, through the three presentations that follow, we begin to explore these issues more fully, as well as consider what is “reasonable,” effective, and the best use of scarce law enforcement resources in sentencing and mitigating cyber crime. There are more questions in this area than can be addressed here, but the conference marks the beginning of a dialogue. Although there has been a significant amount of scholarly work on sentencing and cyber crime, few scholars have expertise in both subjects. In my view, the conference provides (outside of sentencing commission deliberations) one of the first ever explorations of the special issues arising from the intersection of sentencing and cyber crime. In short, what can we do and what should we do with cyber criminals after apprehension and adjudication, and why?