

Chapter 10: Criminal Law and Cyber Crime Prosecuting Cyber Crime
Book Title: Business Law
Printed By: Demond Tibbs (dtibbs@svsu.edu)
© 2015, 2012 Cengage Learning, Cengage Learning

Prosecuting Cyber Crime

Cyber crime has raised new issues in the investigation of crimes and the prosecution of offenders. Determining the “location” of a cyber crime and identifying a criminal in cyberspace present significant challenges for law enforcement.


Jurisdiction and Identification Challenges

A threshold issue is, of course, jurisdiction. Jurisdiction is normally based on physical geography, as discussed in [Chapter 2](#). Each state and nation has jurisdiction, or authority, over crimes committed within its boundaries. But geographic boundaries simply do not apply in cyberspace. A person who commits an act against a business in California, where the act is a cyber crime, might never have set foot in California but might instead reside in New York, or even in Canada, where the act may not be a crime.

Identifying the wrongdoer can also be difficult. Cyber criminals do not leave physical traces, such as fingerprints or DNA samples, as evidence of their crimes. Even electronic “footprints” can be hard to find and follow. For instance, e-mail may be sent through a remailer, an online service that guarantees that a message cannot be traced to its source.

For these reasons, laws written to protect physical property are often difficult to apply in cyberspace. Nonetheless, governments at both the state and the federal level have taken significant steps toward controlling cyber crime. California, for instance, which has the highest identity theft rate in the nation, has established a new eCrime unit to investigate and prosecute cyber crimes. Other states, including Florida, Louisiana, and Texas, also have special law enforcement units that focus solely on Internet crimes.

The Computer Fraud and Abuse Act

Perhaps the most significant federal statute specifically addressing cyber crime is the Counterfeit Access Device and Computer Fraud and Abuse Act.  This act is commonly known as the Computer Fraud and Abuse Act (CFAA).

Among other things, the CFAA provides that a person who accesses a computer online, without authority, to obtain classified, restricted, or protected data (or attempts to do so) is subject to criminal prosecution. Such data could include financial and credit records, medical records, legal files, military and national security files, and other confidential information. The data can be located in government or private computers. The crime has two elements: accessing a computer without authority and taking the data.

This theft is a felony if it is committed for a commercial purpose or for private financial gain, or if the value of the stolen data (or computer time) exceeds \$5,000. Penalties include fines

and imprisonment for up to twenty years. A victim of computer theft can also bring a civil suit against the violator to obtain damages, an injunction, and other relief.

Reviewing: Criminal Law and Cyber Crime

Edward Hanousek worked for Pacific & Arctic Railway and Navigation Company (P&A) as a roadmaster of the White Pass & Yukon Railroad in Alaska. Hanousek was responsible “for every detail of the safe and efficient maintenance and construction of track, structures and marine facilities of the entire railroad,” including special projects. One project was a rock quarry, known as “6-mile,” above the Skagway River. Next to the quarry, and just beneath the surface, ran a high-pressure oil pipeline owned by Pacific & Arctic Pipeline, Inc., P&A’s sister company. When the quarry’s backhoe operator punctured the pipeline, an estimated 1,000 to 5,000 gallons of oil were discharged into the river. Hanousek was charged with negligently discharging a harmful quantity of oil into a navigable water of the United States in violation of the criminal provisions of the Clean Water Act (CWA). Using the information presented in the chapter, answer the following questions.

1. Did Hanousek have the required mental state (*mens rea*) to be convicted of a crime? Why or why not?
2. Which theory discussed in the chapter would enable a court to hold Hanousek criminally liable for violating the statute if he participated in, directed, or merely knew about the specific violation?
3. Could the backhoe operator who punctured the pipeline also be charged with a crime in this situation? Explain.
4. Suppose that at trial, Hanousek argued that he should not be convicted because he was not aware of the requirements of the CWA. Would this defense be successful? Why or why not?

DEBATE THIS... *Because of overcriminalization, particularly by the federal government, Americans may be breaking the law regularly without knowing it. Should Congress rescind many of the more than four thousand federal crimes now on the books?*

© 2018 Cengage Learning Inc. All rights reserved. No part of this work may be reproduced or used in any form or by any means - graphic, electronic, or mechanical, or in any other manner - without the written permission of the copyright holder.