



Enforcing Intellectual Property Rights Through Criminal Prosecution



Special Agent Frederick Pflueger, FBI,
Stephen Ingraham, AUSA and Computer Hacking and
Intellectual Property (CHIP) Coordinator – Eastern District of
Wisconsin and
Timothy O’Shea, AUSA and CHIP – Western District of
Wisconsin



INTRODUCTION

- Intellectual property industries accounted for \$300 billion or almost 4% of U.S. Gross Domestic Product (GDP)
- This value will increase as U.S. industrial economy shifts to an information-based economy
- U.S. leads the world in creation and export of intellectual property



WHY CRIMINALLY PROSECUTE MISAPPROPRIATION OF IP?

- Multi-billion dollar drain on U.S. economy
- Deprives legitimate owners of substantial revenue and goodwill
- Poses health and safety threats to consumers
- To deter and punish misappropriation



Investigative Process



- An intellectual property case starts the same way as any other case; the FBI is notified by the victim, victim's attorney, press, a tip or other law enforcement officer
- Initially, non-intrusive contact is made by an agent or agents to determine whether FBI should investigate further
- If a matter warrants investigation, FBI agents will collect evidence, to include:
 - > interviews
 - > crime scene processing (to include computer and electronic forensics) and
 - > possible undercover operations



When target is identified:

- FBI continues to gather evidence, to include securing search warrants, grand jury testimony/subpoenas
- Subject interviews
- Possible sting operations (perhaps involving consensual monitored telephone calls or meetings)

Investigations are coordinated with U.S. Attorney's Office with the goal of securing convictions.

Part of the consultation between FBI agents and federal prosecutors is to discuss the elements of the crime under investigation



Pluses and minuses

Negative: lose exclusive control of case. This concern is, however, mitigated by consultation with agents and prosecution.

Perceived negative: publicity.

In fact: negative publicity minimized or eliminated because consultation between agents, prosecutors and victims regarding the message results in victim being accurately portrayed as good corporate citizen.



Positives:

Law enforcement has investigative resources not available to civil attorneys:

Search warrants;

Grand Jury process—records and compelled investigative testimony; and

Badges, battering rams & guns.



Positives:

Criminal process has remedies unavailable to civil attorneys:

- prisons;
- Mandatory, non-dischargeable restitution; and
- different sense of vindication for client



COMMONLY CHARGED IP CRIMES

- Trafficking in Counterfeit Goods or Services
- Criminal Copyright Infringement
- Trafficking in Counterfeit Labels

Kah Choon Chay

FBI case

Sentenced to 8 months in prison and
ordered to pay \$49,941.02 in restitution

- Theft of Trade Secrets



COMMONLY CHARGED IP CRIMES

- Other commonly charged federal crimes
 - Federal Mail & Wire Fraud
 - Prohibition on Devices to Intercept Communications
 - Unauthorized Reception of Cable Service
 - Obtaining Information in Excess of Authorization by Means of a Protected Computer
 - Access of a Protected Computer with Intent to Defraud & Obtaining Something of Value



OVERVIEW
OF
CRIMINAL
INTELLECTUAL
PROPERTY LAWS



CRIMINAL TRADEMARK COUNTERFEITING—ELEMENTS

1. Defendant intentionally trafficked or attempted to traffic in goods or services;
2. knowingly used a counterfeit mark on or in connection with counterfeits;
3. mark was registered for thing counterfeited; &
4. mark was in use at time of counterfeiting.

18 USC § 2320(a)



CRIMINAL TRADEMARK COUNTERFEITING—PENALTIES

- Individuals
 - First offense: 10-year felony; \$2 million maximum fine
 - Second offense: 20-year felony; \$5 million maximum fine
- Businesses
 - First offense: \$5 million maximum fine
 - Second offense: \$15 million maximum fine



CRIMINAL COPYRIGHT INFRINGEMENT — ELEMENTS

1. Existence of a copyright;
2. Defendant infringed on the copyright (by reproduction or distribution);
3. Infringement was willful; and
4. (a) For purposes of commercial advantage or private financial gain;
OR
(b) Infringed more than 10 copies with total retail value of more than \$1,000 (misdemeanor) or \$2,500 (felony) within 180 days.

17 USC §506(a) and 18 USC §2319



CRIMINAL COPYRIGHT INFRINGEMENT – DEFENSES

- Fair use defense
 - Excepts an otherwise infringing use where it is used for purposes such as criticism, comment, news, reporting, teaching, scholarship and research. Limits owner's exclusive rights to distribute copies of a copyrighted work to the public to their "first sale" under 17 U.S.C. § 107
- First sale defense
 - Limits owner's exclusive rights to distribute copies of a copyrighted work to the public to their "first sale" under 17 U.S.C. § 106(3)



CRIMINAL COPYRIGHT INFRINGEMENT — PENALTIES

- Misdemeanors: not more than one year and \$100,000 fine
- Basic felony copyright infringement: 3 years and \$250,000 fine
- When for purpose of commercial advantage or financial gain: 5 yrs and \$250,000 fine
- Second offense: 10 years and \$250,000 fine



COUNTERFEIT LABELING— ELEMENTS & PENALTIES

- Defendant knowingly traffics in:
 - Labels to be affixed to audiovisual, literary, or visual works, computer program or its documentation or packaging

18 U.S.C. § 2318

- Penalty: 5 Years



DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) – ELEMENTS & PENALTIES

Elements

1. Defendant trafficked in or used certain methods to circumvent technological measures that protect copyrighted works;
2. Defendant did so willfully; and
3. for commercial advantage or private financial gain

18 USC §§ 1201 and 1204

Penalties:

- First offense: 5 Years, \$500,000 Fine
- Repeat offenses: 10 Years, \$1,000,000 Fine



DMCA – DEFENSES

- Exempted classes of works
- Government investigative, protective, information security, intelligence
- Reverse-engineering to make computer programs interoperable
- Encryption research
- Restricting minors' access to Internet
- Protect personally identifying information
- Security testing
- Nonprofit libraries, archives, educational institutions, or public broadcasting entities



THEFT OF TRADE SECRETS— ELEMENTS

1. Defendant obtained, destroyed, received or conveyed information;
2. without the owner's authorization;
3. knowing or believing that the information was a trade secret;
4. knowing or intending that owner would be injured;
5. the information was related to product in interstate or foreign commerce; and
6. defendant intended to convert trade secret to economic benefit of someone other than the owner



ECONOMIC ESPIONAGE— ELEMENTS

1. Defendant obtained, destroyed, received or conveyed information;
2. without the owner's authorization;
3. defendant knew or believed information was a trade secret; and
4. Defendant knew or believed offense would benefit a foreign government, instrumentality, or agent



THEFT OF TRADE SECRETS & ECONOMIC ESPIONAGE— PENALTIES

- Trade Secrets: 10 years and \$5 million for organization
- Economic Espionage: 15 years and \$10 million for organization
- Forfeiture and destruction of illegal products



THEFT OF TRADE SECRETS & ECONOMIC ESPIONAGE

- US v. Kissane (2002) — 24 months jail for ex-employee who offered to sell the source code of his ex-employer to competitors



PROSECUTORIAL POLICY CONSIDERATIONS

- Strength of the evidence
- Nature and seriousness of the offense
 - Magnitude and scope
 - Health and safety risks
 - Deterrent effect on individual's future conduct
- Possible defenses
- Jury's likely response



PROSECUTORIAL POLICY CONSIDERATIONS

- Person's culpability in the offense
- Person's criminal history
- Person's history of criminal and civil IP violations
- Person's willingness to cooperate in investigating and prosecution of others
- Person's probable sentence or other consequences of conviction



PROSECUTORIAL POLICY CONSIDERATIONS

- Deterrent effect of prosecution
- Federal law enforcement priorities
- Adequacy of non-criminal alternatives to prosecution
 - Asset forfeiture by the government
 - Civil suits by the victims



PUBLICATIONS

- *Prosecuting Intellectual Property Crimes (2001)*
- *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2002)*
- www.cybercrime.gov



QUESTIONS?



Contact Information:

Timothy O'Shea

(608) 264-5158, tim.oshea@usdoj.gov

U.S. Attorneys Office for the Western District of Wisconsin