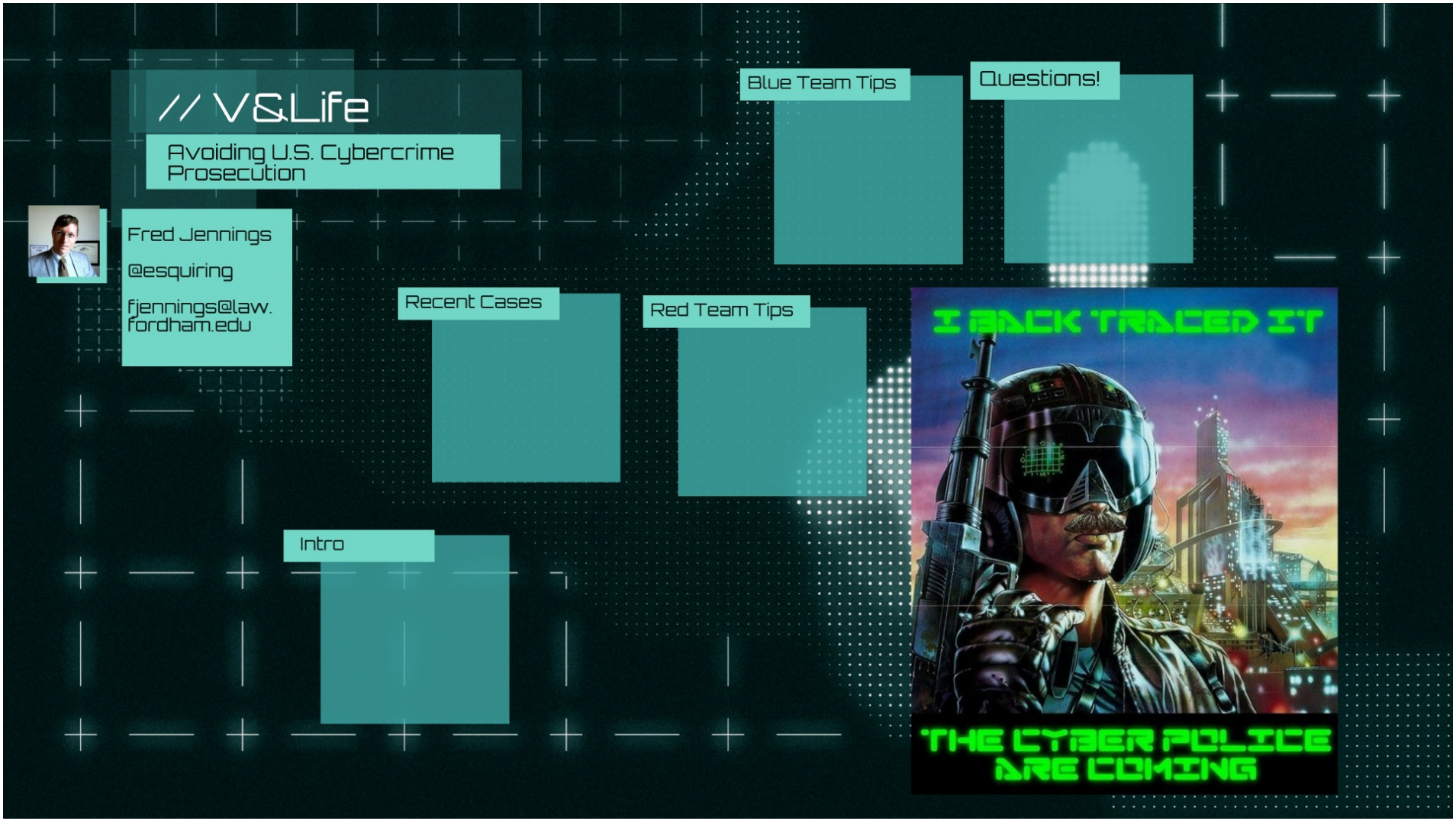

// V&Life
Avoiding U.S. Cybercrime Prosecution
Fred Jennings
@esquiring
fjennings@law.fordham.edu
Intro
Recent Cases
Red Team Tips
Blue Team Tips
Questions!
I BACK TRACED IT
THE CYBER POLICE ARE COMING

Who / What / Why

- Who am I?
- What are we talking about?
- Why do you care?

TABLE OF CONTENTS

Section		Page
1.0	**INTRODUCTION**	**1**
2.0	**ORGANIZATIONAL AND SOCIAL CONSIDERATIONS**	**1**
2.1	Terminology	2
2.1.1	Hackers	2
2.1.2	Crackers	2
2.1.3	Warez Dudez	3
2.1.4	Phreaks	3
2.2	Communication Mechanisms	3
2.2.1	Bulletin Board Systems (BBS)	3
2.2.2	Newsgroups	4
2.2.3	Mailing Lists	5
2.2.4	Internet Relay Chat	6

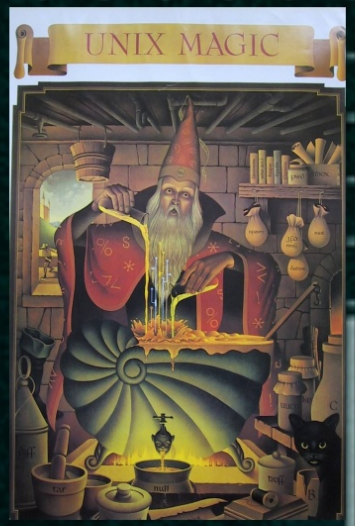
What's the CFAA?

A Note on Laws

What's the C.F.A.A.?

- Passed in 1984
  (though amended since, most recently in 2020)
- Creates standalone crimes for "unauthorized access" and "unauthorized damage"
- Very broad language means many innocent and necessary research tasks can fall under its reach
- Note recent(ish) DoJ guidance

DoJ Guidance



DoJ Guidance

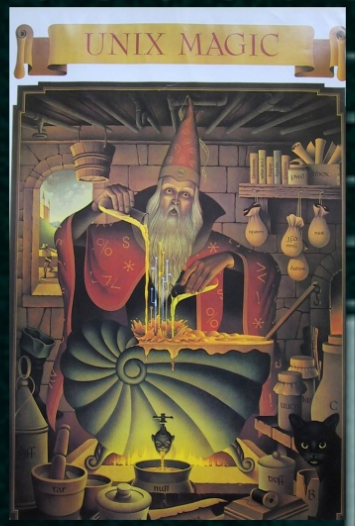
A. *Policy*. In addition to the considerations set forth in JM § 9-27.230, which are incorporated herein by reference, an attorney for the Department of Justice should consider the following additional factors in determining whether prosecution of a violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, should be pursued because a substantial federal interest would be served by prosecution in a case in which the admissible evidence is expected to be sufficient to sustain a conviction. It is recognized that the significance of any cyber event for a District can vary depending on facts and circumstances specific to the District. Factors to be considered include:

1. The sensitivity of the affected computer system or the information transmitted by or stored on it and the likelihood and extent of harm associated with damage or unauthorized access to the computer system or related disclosure and use of information;
2. The degree to which damage or access to the computer system or the information transmitted by or stored on it raises concerns pertaining to national security, critical infrastructure, public health and safety, market integrity, international relations, or other considerations having a broad or significant impact on national or economic interests;
3. The extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm or a threat to national security;
4. The impact of the crime and prosecution on the victim or other third parties;
5. Whether the criminal conduct is based upon exceeding authorized access consistent with the policy set forth in Section B(5) below;
6. The deterrent value of an investigation or prosecution, including whether the need for deterrence is increased because the activity involves a new or expanding area of criminal activity, a recidivist defendant, use of a novel or sophisticated technique, or abuse of a position of trust or otherwise sensitive level of access, or because the conduct is particularly egregious or malicious;
7. The nature of the impact that the criminal conduct has on a particular District or community; and,
8. Whether any other jurisdiction is likely to prosecute the criminal conduct effectively, if the matter is declined for federal prosecution.

What's the C.F.A.A.?

- Passed in 1984
  (though amended since, most recently in 2020)
- Creates standalone crimes for "unauthorized access" and "unauthorized damage"
- Very broad language means many innocent and necessary research tasks can fall under its reach
- Note recent(ish) DoJ guidance

DoJ Guidance



Who / What / Why

- Who am I?
- What are we talking about?
- Why do you care?

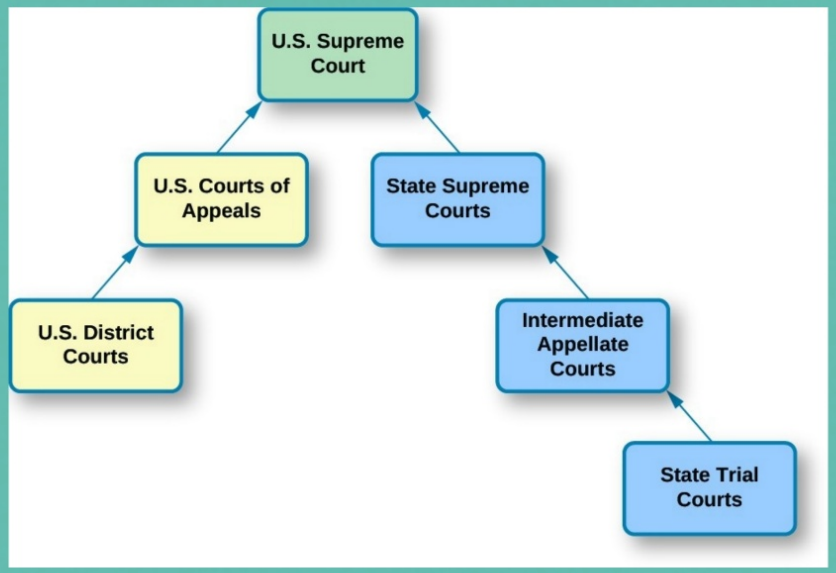
TABLE OF CONTENTS

Section		Page
1.0	**INTRODUCTION**	**1**
2.0	**ORGANIZATIONAL AND SOCIAL CONSIDERATIONS**	**1**
2.1	Terminology	2
2.1.1	Hackers	2
2.1.2	Crackers	2
2.1.3	Warez Dudez	3
2.1.4	Phreaks	3
2.2	Communication Mechanisms	3
2.2.1	Bulletin Board Systems (BBS)	3
2.2.2	Newsgroups	4
2.2.3	Mailing Lists	5
2.2.4	Internet Relay Chat	6

What's the CFAA?

A Note on Laws

A Note on Laws



Who / What / Why

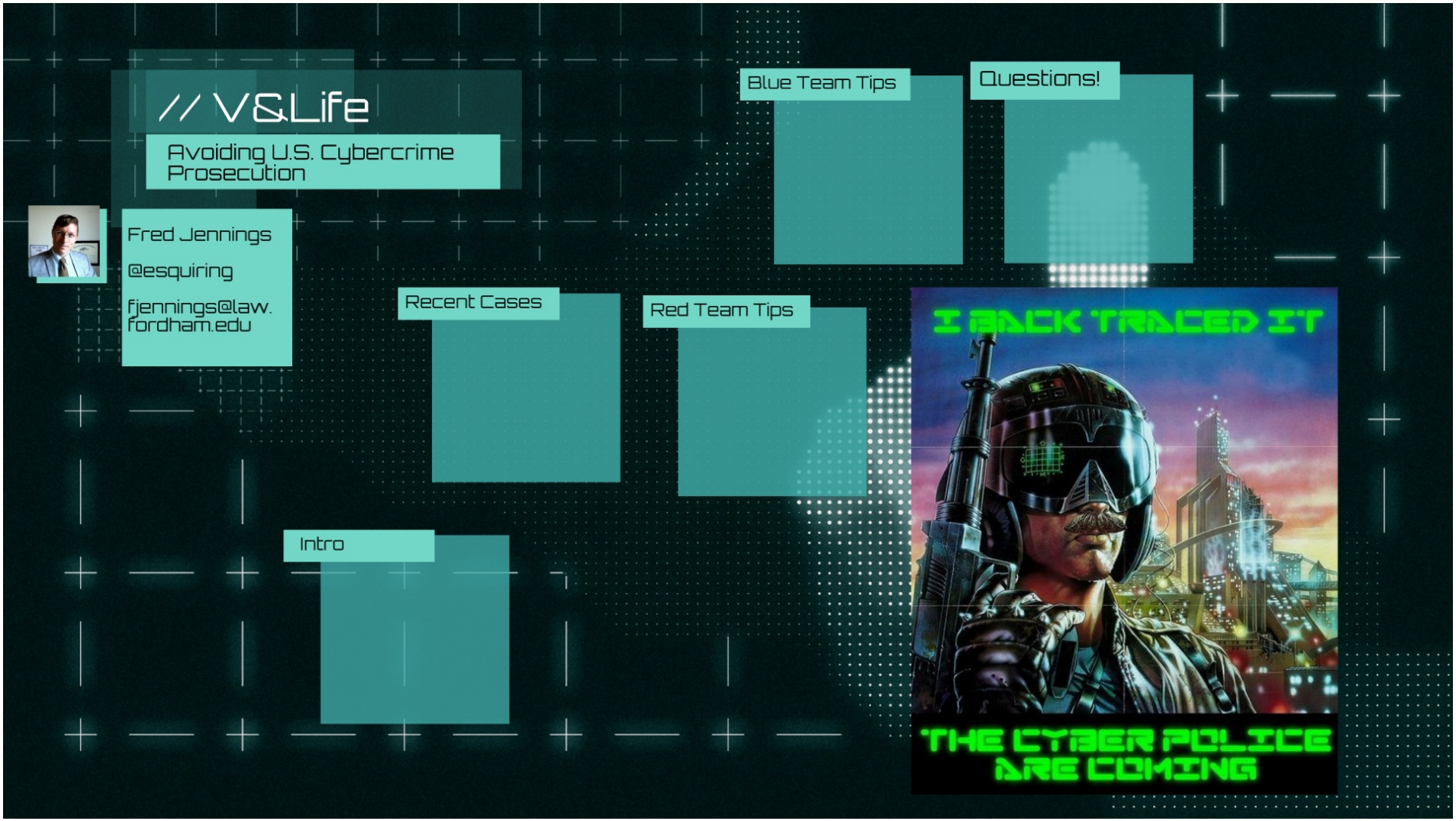
- Who am I?
- What are we talking about?
- Why do you care?

TABLE OF CONTENTS

Section		Page
1.0	**INTRODUCTION**	**1**
2.0	**ORGANIZATIONAL AND SOCIAL CONSIDERATIONS**	**1**
2.1	Terminology	2
2.1.1	Hackers	2
2.1.2	Crackers	2
2.1.3	Warez Dudez	3
2.1.4	Phreaks	3
2.2	Communication Mechanisms	3
2.2.1	Bulletin Board Systems (BBS)	3
2.2.2	Newsgroups	4
2.2.3	Mailing Lists	5
2.2.4	Internet Relay Chat	6

What's the CFAA?

A Note on Laws


// V&Life
Avoiding U.S. Cybercrime Prosecution
Fred Jennings
@esquiring
fjennings@law.fordham.edu
Intro
Recent Cases
Red Team Tips
Blue Team Tips
Questions!
I BACK TRACED IT
THE CYBER POLICE ARE COMING

Recent Cases

- Sandvig v. Barr
  1:16 cv 1368 (D.D.C. 2016)
- Van Buren v. United States
  19-783 (SCOTUS)
- United States v. Marcus Hutchins
  17 cr (E.D. Wis. 2017)

Hutchins allegedly updated the Kronos malware, and distributed it to Individual B, who was located in California and was known to be involved in cyber-based criminal activities.

On July 11, 2017, a grand jury indicted Hutchins on various counts

// V&Life

Avoiding U.S. Cybercrime Prosecution

Fred Jennings

@esquiring

fjennings@law.fordham.edu

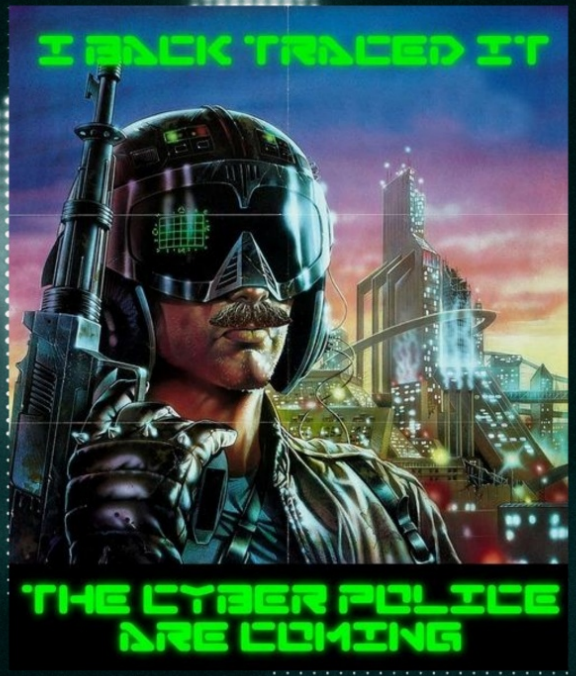
Blue Team Tips

Questions!

Recent Cases

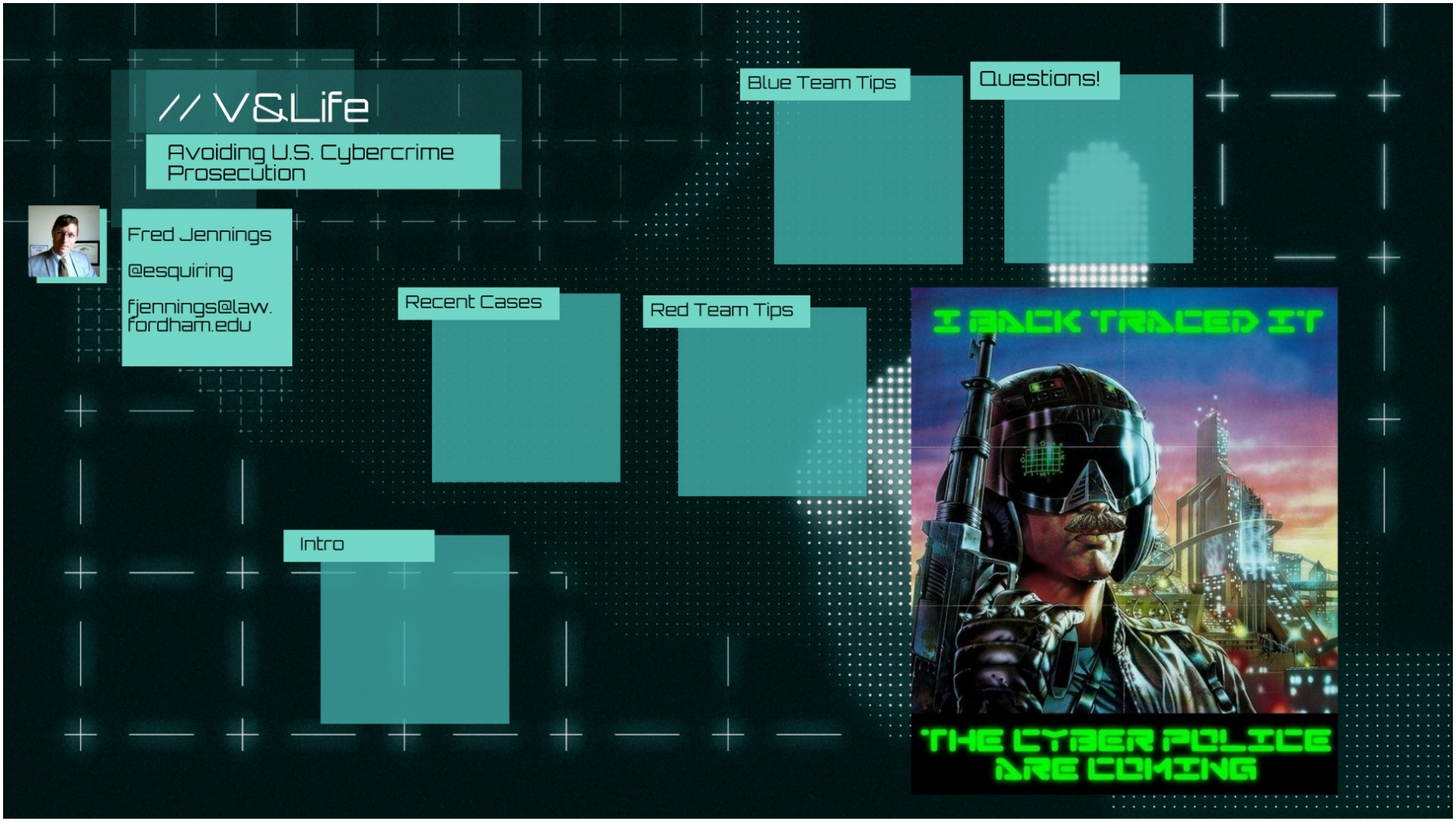
Red Team Tips

Intro



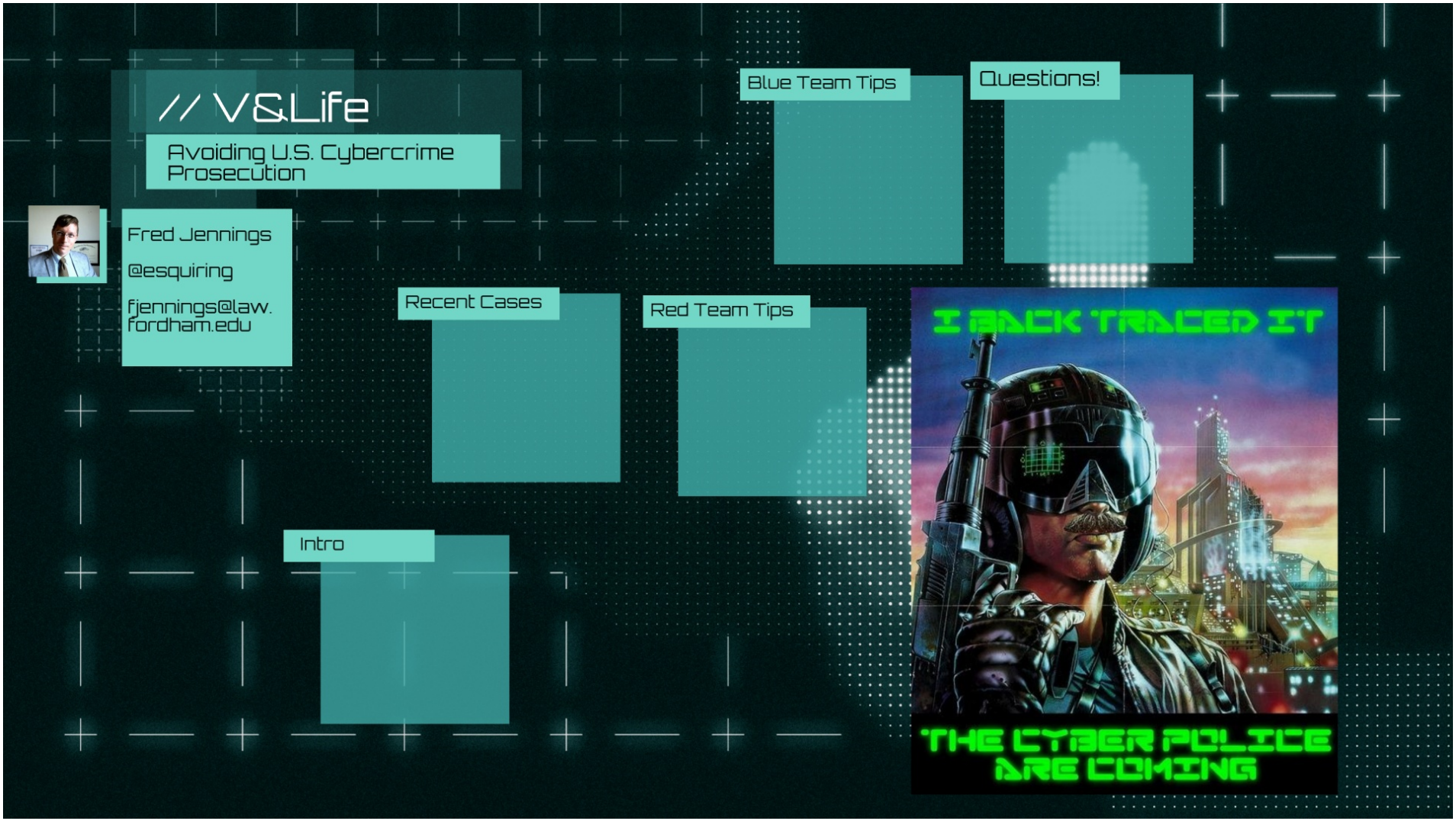
Red Team Tips

- FFS have a contract
- Be sure that contract has clear Scope of Engagement and "Get Out of Jail" sections
- If you're exceeding that scope on engagement, watch out.
- Apply similar caution to bug bounty terms, etc.


// V&Life
Avoiding U.S. Cybercrime Prosecution
Fred Jennings
@esquiring
fjennings@law.fordham.edu
Intro
Recent Cases
Red Team Tips
Blue Team Tips
Questions!
I BACK TRACED IT
THE CYBER POLICE ARE COMING

Blue Team Tips

- Are your defensive tools purely defensive?
- If you have a bug bounty, or engage outside researchers, do those Terms cover CFAA indemnity?
- Consider a conversation with company Legal about whether, when, and how law enforcement is engaged with.
- Company advocacy can drive reform - this goes for all flavors of security orgs.


// V&Life
Avoiding U.S. Cybercrime Prosecution
Fred Jennings
@esquiring
fjennings@law.fordham.edu
Intro
Recent Cases
Red Team Tips
Blue Team Tips
Questions!
I BACK TRACED IT
THE CYBER POLICE ARE COMING

Q & A

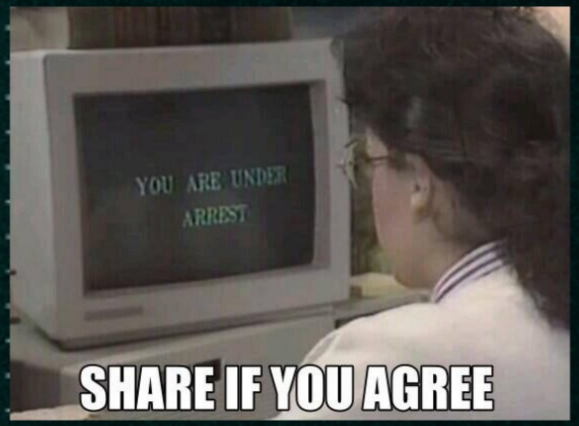
- The CFAA's Breadth is a Danger to Researchers
- Don't Talk to the F*&king Cops Without a Lawyer
- Questions?

Contact info:

Fred Jennings
(admitted in New York, the 2nd Circuit Court of Appeals, and the Supreme Court of the United States)

Twitter: @Esquiring

fjennings@law.fordham.edu



// V&Life

Avoiding U.S. Cybercrime Prosecution

Fred Jennings

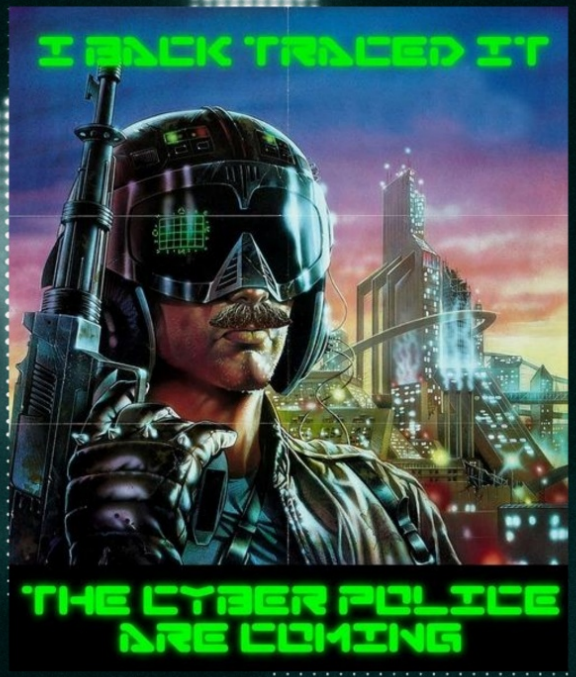
@esquiring

fjennings@law.fordham.edu

Intro

Recent Cases

Red Team Tips

Blue Team Tips

Questions!