

**Computer Crimes Seminar**  
**Spring 2023 Syllabus**

**Professors**

Josh Goldfoot  
[jgoldfoo@gmu.edu](mailto:jgoldfoo@gmu.edu)

Kellen Dwyer  
[kdwyer8@gmu.edu](mailto:kdwyer8@gmu.edu)

**Office hours**

Immediately following class or by appointment

**Grading**

Your grade will be based on a paper addressing an approved topic related to the class (85% of the grade) and your presentation to the class regarding your paper (15% of the grade), subject to a discretionary single-increment adjustment either upward or downward for class participation (e.g., from B to B+ or from A- to B+).

**Part I: Charging Cybercrime**

**January 17 -- Overview of Computer Intrusions and Security**

Indictment in *United States v. Viktor Borisovich Netyksho et al.*, available at <https://www.justice.gov/archives/sco/file/1080281/download>

**January 24 -- Computer Fraud and Abuse Act (CFAA)**

18 U.S.C. 1030(a), (b)

*Van Buren v. United States*, 141 S. Ct. 1648 (2021)

Department of Justice Computer Fraud and Abuse Act Charging Policy, May 2022, <https://www.justice.gov/opa/press-release/file/1507126/download>

*hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022)

**January 31 – Conspiracy and Aiding and Abetting Online**

*United States v. Ulbricht*, 31 F.Supp.3d 540 (S.D.N.Y. 2014) (Silk Road case).

Kevin Paulson, *FBI Arrests Hacker Who Hacked No One*, *Daily Beast* (Mar. 31, 2017), <https://www.thedailybeast.com/fbi-arrests-hacker-who-hacked-no-one>

*United States v. Bondars*, 801 Fed.Appx. 872 (4th Cir. 2020), <https://www.ca4.uscourts.gov/opinions/184718.U.pdf>

Kellen Dwyer, *It's Time to Surge Resources into Prosecuting Ransomware Gangs* (LawFare, May 20, 2021), <https://www.lawfareblog.com/its-time-surge-resources-prosecuting-ransomware-gangs>

## **February 7 – Cryptocurrency, Ransomware, and the DarkWeb: Criminal Uses and Government Responses**

### Ransomware:

Indictment in *United States v. Yaroslav Vasinskyi*, <https://www.justice.gov/opa/press-release/file/1447126/download>

### Dark Web and Online Operations:

*United States v. Eldred*, 933 F.3d 110 (2d Cir. 2019) (“Playpen” operation)

Fed. R. Crim. P. 41(b)(6)

### Cryptocurrency:

Department of Justice, *Cryptocurrency Enforcement Framework* <https://www.justice.gov/archives/ag/page/file/1326061/download> (from page 2, “The basics,” through page 22)

Department of Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (September 21, 2021) [https://home.treasury.gov/system/files/126/ofac\\_ransomware\\_advisory.pdf](https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf)

Treasury Department, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange* (Nov. 8, 2021), <https://home.treasury.gov/news/press-releases/jy0471>

## Part II: Investigating Cybercrime

### February 14 – Obtaining Prospective Communications From Providers

#### 1. Pen-trap Act

- *Smith v. Maryland*, 442 U.S. 735 (1979)
- *In Matter of Application of U.S. For an Ord. Authorizing the Installation & Use of a Pen Reg. & a Trap & Trace Device on E-Mail Acct.*, 416 F. Supp. 2d 13 (D.D.C. 2006)

#### 2. Wiretap Act

- Department of Justice, Electronic Surveillance Manual, available at <https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf> (part III, PDF pages 10-23 only)
- *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010)

#### 3. Foreign Intelligence Surveillance Act

- *United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 308–24 (1972)
- Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, at 1-16 (introduction and executive summary only) (available at <https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf>)

### February 21 – Obtaining Stored Records and Communications From Providers

Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 G.W. L. Rev. 1208, 1208-1224 (2004), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=421860](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860)

#### 1. Contents of communications

- *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (e-mail)
- *People v. Harris*, 36 Misc. 3d 868, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012) (tweets)

#### 2. Location Information

- *Carpenter v. United States*, 138 S. Ct. 2206 (2018)

### 3. Basic Subscriber Information

- *Sams v. Yahoo! Inc.*, 713 F.3d 1175 (9th Cir. 2013)

## **February 28 – Computer Search and Seizure**

Fed. Rule Criminal Procedure 41(e)(2)

*United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016) (forensic review of a computer)

*Riley v. Calif.*, 573 U.S. 373 (2014) (seizure incident to arrest)

Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berk. J. Crim. L. 112 (2010), available at <https://lawcat.berkeley.edu/record/1124398> .

Alex Iftimie, No Server Left Behind: The Justice Department’s Novel Law Enforcement Operation to Protect Victims. Lawfare (Apr. 19, 2021), <https://www.lawfareblog.com/no-server-left-behind-justice-departments-novel-law-enforcement-operation-protect-victims>

## **March 7– Encryption**

Ellen Nakashima, *Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks* (WaPo. Feb. 18, 2016)

<https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-CDCal-Apple-Reply.pdf>  
(Apple brief in San Bernardino case)

<https://www.justice.gov/usao-cdca/file/832166/download> (government brief in San Bernardino case))

Remarks of Attorney General William Barr at Lawful Access Summit (Oct. 4, 2019)

<https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawfulaccess-summit>

Remarks of FBI Director Christopher Wray at the Lawful Access Summit (Oct. 4, 2019)

<https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access>

Susan Landau, [Exceptional Access: The Devil is in the Details](#) (LawFare, Dec. 26, 2018)

Apple v. NSO Group, (N.D. Cal. 2021),  
[https://www.apple.com/newsroom/pdfs/Apple v NSO Complaint\\_112321.pdf](https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf)

*Internal Documents Show How Close the FBI Came to Deploying Spyware* (N.Y. Times Nov. 15, 2022), <https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html>

### **March 14 – Spring Break**

### **March 21 – Network Defense, Information Sharing, and Law Enforcement Cooperation**

Department of Justice/CCIPS, Best Practices for Victim Response and Reporting of Cyber Incidents, Version 2.0, available at <https://www.justice.gov/criminal-ccips/file/1096971/download>

Department of Justice & Department of Homeland Security, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, available at [https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015\\_1.pdf](https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf).

CSIS/DOJ Active Cyber Defense Experts Roundtable March 10, 2015, *available at* <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf>

CCIPS, [Legal Considerations When Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources](https://www.justice.gov/criminal-ccips/page/file/1252341/download), <https://www.justice.gov/criminal-ccips/page/file/1252341/download>

Kellen Dwyer, [The Fallout from the First Trial of a Corporate Executive for ‘Covering Up’ a Data Breach](https://www.lawfareblog.com/fallout-first-trial-corporate-executive-covering-data-breach), *Lawfare* (Oct. 19, 2022), <https://www.lawfareblog.com/fallout-first-trial-corporate-executive-covering-data-breach>

### **III. International Cyber Threats**

### **March 28 -- Foreign Election Interference, Content Moderation, and Section 230**

*United States v. Internet Research Agency et al.*, <https://www.justice.gov/file/1035477/download>

Department of Justice, *Report of the Attorney General’s Cyber-Digital Task Force*, <https://www.justice.gov/archives/ag/page/file/1076696/download> (Read Chapter 1: Countering Malign Foreign Influence Operations)

Justice Manual, 9-90.730, “Disclosure of Foreign Influence Operations,”  
<https://www.justice.gov/jm/jm-9-90000-national-security#9-90.730>

Peter Machtiger, *The Latest GRU Indictment: A Failed Exercise in Deterrence* (Oct. 29, 2020),  
<https://www.justsecurity.org/73071/the-latest-gru-indictment-a-failed-exercise-in-deterrence/>

Ellen Nakashima, Overstating the foreign threat to elections poses its own risks, U.S. officials and experts say, Wash. Post (Oct. 29, 2020), at [https://www.washingtonpost.com/national-security/foreign-interference-threat-elections-overestimated/2020/10/29/387d4640-17e7-11eb-82db-60b15c874105\\_story.html](https://www.washingtonpost.com/national-security/foreign-interference-threat-elections-overestimated/2020/10/29/387d4640-17e7-11eb-82db-60b15c874105_story.html)

[Gonzalez v. Google \(cert granted, Oct. 3, 2022\) \(read cert. Petition, skim merits briefs\).](https://www.scotusblog.com/case-files/cases/gonzalez-v-google-llc/)  
<https://www.scotusblog.com/case-files/cases/gonzalez-v-google-llc/>

[Netchoice v. Paxton \(5<sup>th</sup> Cir. 2022\), https://www.ca5.uscourts.gov/opinions/pub/21/21-51178-CV1.pdf](https://www.ca5.uscourts.gov/opinions/pub/21/21-51178-CV1.pdf)

#### **April 4 – Data Wars, Data Diplomacy, and the Balkanization of the Internet**

*Matter of Warrant to Search a Certain E-Mail Acct. Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), *vacated and remanded sub nom. United States v. Microsoft Corp.*, 138 S. Ct. 1186, 200 L. Ed. 2d 610 (2018)

18 U.S.C. § 2713, 2703(h) (CLOUD Act, enacted March 23, 2018)

Department of Justice CLOUD Act FAQ,  
<https://www.justice.gov/dag/page/file/1153466/download>

*Schrems II a summary - all you need to know* (GDPR Summary), available at  
<https://www.gdprsummary.com/schrems-ii/>

Office of National Intelligence et al, *Information on US Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-US Data Transfers after Schrems II* (Sept. 23, 2020), available at <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>

*U.S. and European leaders reach deal on trans-Atlantic data privacy* (NY Times, Mar. 25, 2022)  
<https://www.nytimes.com/2022/03/25/business/us-europe-data-privacy.html>

Executive Order to Implement the European Union-US. Data Privacy Framework (Oct. 7, 2022),  
<https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/>

[The 2018 DOD Cyber Strategy: Understanding ‘Defense Forward’ in Light of the NDAA and PPD-20 Changes](#) (LawFare Sept. 25, 2018)

Bobby Chesney, Sanctioning Russia for SolarWinds: What Normative Line Did Russia Cross, LawFare (April 15, 2021), <https://www.lawfareblog.com/sanctioning-russia-solarwinds-what-normative-line-did-russia-cross>

Michael Ellis, For Cybersecurity, the Best Defense is a Good Offense (Heritage Institute, Nov. 10, 2021), <https://www.heritage.org/technology/report/cybersecurity-the-best-defense-good-offense>

### **April 11 & 18 – Paper presentations**

Paper Presentations Due

### **April 28 -Final Paper Due**

## **Computer Crimes Seminar**

### **Student Learning Objectives**

- Students will be able to demonstrate knowledge of computer crime cases and the application of relevant laws.
- Students will be able to define the major ideas in computers and technology and criminal laws and be able to identify their interrelationships.
- Students will be able to analyze information about computer crime cases and make judgments about the appropriate application of criminal laws to those cases.
- Students will be able to describe the approaches and underlying values of computer crime law knowledge and case review and apply that knowledge to their practice.
- Students will be able to communicate their knowledge about this subject orally and in writing, to a variety of audiences.
- Students will be able to apply the course information and skills to real world situations.
- Students will be able to reflect on how to discover computer crime laws and their application and can create plans to incorporate that knowledge into their own work practices and case research.