Computer Crimes Seminar
Spring 2022 Syllabus

Professors
Josh Goldfoot
jgoldfoo@gmu.edu

Kellen Dwyer
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 (e.g. from B to B+ or from A- to B+).

Part I: Charging Cybercrime

January 18 -- Overview of Computer Intrusions and Security

Ars Technica, Anonymous speaks: the Inside Story of the HBGary Hack (Feb. 15, 2011), https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

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

January 25 -- Computer Fraud and Abuse Act (CFAA)

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

Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065–69 (9th Cir. 2016)

Department of Justice, Computer Crimes and Intellectual Property Section, *Prosecuting Computer Crimes*, https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ccmanual.pdf
(**skim chapter one** -- we just want you to understand the structure of the CFAA and the elements of the different computer intrusion crimes it created)

James Grimmelmann, *Consenting to Computer Use,* 84 Geo. Wash. L. Rev. 1500 (2016)

February 1 – 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 8 – Cryptocurrency, Ransomware, and the DarkWeb: Criminal Uses and Government Responses

United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020)

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

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

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

February 15 -- Foreign Election Interference

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/1076696/download (Read Chapter 1: Countering Malign Foriegn 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

Deputy Assistant Attorney General Adam Hickey, Remarks at the ACI 2nd National Forum on FARA (Dec. 4, 2020), https://www.justice.gov/opa/speech/deputy-assistant-attorney-generalnational-security-division-adam-hickey-delivers-remarks

Atlantic Council, *Why Foreign Election Interference Fizzled In 2020* (Nov. 23, 2020)

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

Vivek Ramaswamy & Jed Rubenfeld, *Save the Constitution From Big Tech*, Wall St. J. (Jan. 11, 2021), at https://www.wsj.com/articles/save-the-constitution-from-big-tech-11610387105?st=6u9us2nj3njfs22&reflink=desktopwebshare_permalink

Part II: Investigating Cybercrime

February 22 – Obtaining Prospective Communications From Providers

1. Wiretap Act
   - *Berger v. New York*, 388 U.S. 41 (1967) (majority opinion only)
   - 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)

2. 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)

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)

March 1 – 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

1. Basic Subscriber Information

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

2. Location Information

- *Carpenter v. United States*, 138 S. Ct. 2206 (2018)
- Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L. & Tech. 357, 369-385 (2019)

3. 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)

March 8 – Computer Search and Seizure

Fed. Rule Criminal Procedure 41(e)(2)
United States v. Ganias, 824 F.3d 199 (2d Cir. 2016) (forensic review of a computer)
Riley v. Calif., 573 U.S. 373 (2014) (seizure incident to arrest)

United States v. Cotterman, 709 F.3d 952, 961 (9th Cir. 2013) (border search)

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

March 22– 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)

March 29 – 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 .

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

III. International Cyber Threats

April 5 – 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

Center for Democracy and Technology, *Schrems II and the Need for Intelligence Surveillance Reform* (Jan. 13, 2021), *available at* https://cdt.org/wp-content/uploads/2021/01/2021-01-13-CDT-Schrems-II-and-Intelligence-Surveillance-Reform-in-the-US.pdf

The oracle at Luxembourg: The EU Court of Justice judges the world on surveillance and privacy (Brookings Institute, Jan. 11, 2021), https://www.brookings.edu/research/the-oracle-atluxembourg-the-eu-court-of-justice-judges-the-world-on-surveillance-and-privacy/

April 12– Cyber Warfare

Robert Chesney, *U.S. Cyber Command and the Russian Grid: Proportional Countermeasures, Statutory Authorities and Presidential Notification*, Lawfare (June 17, 2019), https://www.lawfareblog.com/us-cyber-command-and-russian-grid-proportionalcountermeasures-statutory-authorities-and

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

Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LawFare (July 26, 2018), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa

Associate Deputy Attorney General Sujit Raman, *The Rule of Law in the Age of Great Power Competition in Cyberspace* https://www.justice.gov/opa/speech/associate-deputy-attorneygeneral-sujit-raman-delivers-remarks-aba-rule-law-initiative

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 19 – 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.