USC Annenberg

JOUR 499 Special Topics: Digital Security for Journalists and Communicators
2 Units

Spring 2020 – Tuesdays – 10-11:40 a.m.
Section: 21371R
Location: ANN 408

Instructors: Marc Ambinder and Josh Campbell
Office: ANN Lobby
Office Hours: TBD/Upon Request
Contact Info: Marc.Ambinder@gmail.com;
JoshuaCampbell@outlook.com

I. Course Description
Right now, you – the person reading this description – are hemorrhaging a trail of personal data that others are eagerly exploiting. If you live and work in the digital dimension, your stuff, your work, your property, your ideas – are highly vulnerable to hacks, attacks, sabotage, and harassment. From foreign governments hacking into production servers, to the spoofing of news articles, competitive theft and online harassment, the information environment is full of snares.

This course is a practical introduction to the essentials of digital security for professional communicators – reporters, public relations strategists, diplomats-in-training, politicians, reporters, speechwriters, communications managers and directors, brand influencers, press spokespeople – really, anyone whose job requires them to protect intellectual property, ideas, designs, and concepts, or the integrity of communications between you and your clients or sources.

Students will not only be able to practice better security, but they'll be able to teach those whose lives and livelihoods depends upon the secure transmission of information. This is not a course for engineers. It's a course that uses what computer engineers know about the internet, what spies and hackers know, what the government and big corporations know – and translates those specialized and technical concepts into plain language and ready-to-use tactics to fight against them. It's taught by a renowned investigative journalist and teacher and a former FBI agent, both of whom will distill the best available practices so you can serve your clients, sources, publications, audience and the public more securely and more efficiently, all without cluttering your mind with too much technical gobbledygook.

II. Overall Learning Objectives and Assessment
— Identify threats to the information security environment for communicators
— describe the basic structure of the internet and understand its inherent design flaws, informing their practice – including the vulnerability of the cloud, the layers of the Internet, ISP data collection, service providers, devices, credential verification, digital certificates
— Assess, and reduce their social, digital and personal footprints, as needed
— How to travel abroad (and anywhere near the U.S. border) with sensitive information
— Describe the laws governing search, seizure, access, and communications interception and apply that knowledge to protect their own and others' information
— Use encrypted messenger apps, TOR, VPNs, secure document hubs, 1.1.1.1. to protect their own and others' information
— Analyze information risks in communication scenarios and create strategies to minimize those risks

III. Description of Assignments and Assessment

These assignments form the core of the course. They are designed to let you apply what you've learned in class to real-world problems you may confront. The instructors may change them as warranted. The assessment rubrics will vary based on the nature of the assignment, and they will be made clear to students well in advance of the due dates.

The following exercises will be evaluated:

- Perform a basic risk assessment in advance of meeting with a source at the USC Village
- Identify and interview a practitioner about the security practices they employ
- Installing, using, and teaching others how to use VPNs, TOR and PGP
- Creatively addressing the question about how to use technology without being tracked or identified with that piece of technology
- Reducing/mitigating their own digital footprints and vulnerability

IV. Grading
a. Breakdown of Grade

Assignment	Points	% of Grade
Participation	150	15%
Assignments (6, graded on 100 points)	600	50%
Quizzes	50	10%
Final Exam	250	25%
TOTAL	**1,000**	**100%**

b. Grading Scale

95% to 100%: A	80% to 83%: B-	67% to 69%: D+
90% to 94%: A-	77% to 79%: C+	64% to 66%: D
87% to 89%: B+	74% to 76%: C	60% to 63%: D-
84% to 86%: B	70% to 73%: C-	0% to 59%: F

V. Grading Standards

Because the class is open to all ASCJ students, the assignments will not be graded as if they were professional journalistic work products.

However, because good digital security practices depend upon close observation and attention to detail, assignment write-ups that are hastily assembled or poorly written will be given lower grades. For the risk

assessments, highly-graded assignments will reflect a considered attention to detail, an operational understanding of the material and the scenarios described and the ability to correctly identify and mitigate vulnerabilities.

For reference, the Journalism School standards are included below.

Journalism

All assignments will be edited on a professional basis and you will be judged first on the accuracy, fairness and objectivity of your stories. You will then be evaluated for broadcast style, editing, production value, originality and the ability to meet deadlines.

"A" stories are accurate, clear, comprehensive stories that are well written and require only minor copyediting (i.e., they would be aired or published). Video work must also be shot and edited creatively, be well paced and include good sound bites and natural sound that add flavor, color or emotion to the story.

"B" stories require more than minor editing and have a few style or spelling errors or one significant error of omission. For video, there may be minor flaws in the composition of some shots or in the editing. Good use of available sound bites is required.

"C" stories need considerable editing or rewriting and/or have many spelling, style or omission errors. Camera work and editing techniques in video stories are mediocre or unimaginative, but passable. Sound bites add little or no color - only information that could be better told in the reporter's narration.

"D" stories require excessive rewriting, have numerous errors and should not have been submitted. Camera work is unsatisfactory or fails to show important elements.

"F" stories have failed to meet the major criteria of the assignment, are late, have numerous errors or both. Your copy should not contain any errors in spelling, style, grammar and facts. Any misspelled or mispronounced proper noun will result in an automatic "F" on that assignment. Any factual error will also result in an automatic "F" on the assignment. Accuracy is the first law of journalism. The following are some other circumstances that would warrant a grade of "F" and potential USC/Annenberg disciplinary action:

- Fabricating a story or making up quotes or information.
- Plagiarizing a script/article, part of a script/article or information from any source.
- Staging video or telling interview subjects what to say.
- Using video shot by someone else and presenting it as original work.
- Shooting video in one location and presenting it as another location.
- Using the camcorder to intentionally intimidate, provoke or incite a person or a group of people to elicit more "dramatic" video.
- Promising, paying or giving someone something in exchange for doing an interview either on or off camera.
- Missing a deadline.

VI. Assignment Submission Policy

Assignments must be submitted via BLACKBOARD or directly to the instructor(s) by the due date UNLESS OTHERWISE INSTRUCTED.

VII. Required Readings and Supplementary Materials

Please purchase the following book:

Bruce Schneiner, Click Here, (available on Amazon for about ten bucks)

VIII. Laptop Policy

All undergraduate and graduate Annenberg majors and minors are required to have a PC or Apple laptop that can be used in Annenberg classes. Please refer to the **Annenberg Digital Lounge** for more information. To connect to USC's Secure Wireless network, please visit USC's **Information Technology Services** website.

IX. Add/Drop Dates for Session 001 (15 weeks: 1/13/20 – 5/1/20)

Friday, January 31: Last day to register and add classes for Session 001
Friday, January 31: Last day to drop a class without a mark of "W," except for Monday-only classes, and receive a refund for Session 001
Tuesday, February 4: Last day to drop a Monday-only class without a mark of "W" and receive a refund for Session 001
Friday, February 28: Last day to drop a course without a mark of "W" on the transcript for Session 001. [Please drop any course by the end of week three (or the 20 percent mark of the session) to avoid tuition charges.]
Friday, February 28: Last day to change pass/no pass to letter grade for Session 001. [All major and minor courses must be taken for a letter grade.]
Friday, April 3: Last day to drop a class with a mark of "W" for Session 001

X. Course Schedule: A Weekly Breakdown

Important note to students: *Be advised that this syllabus is subject to change - and probably will change - based on the progress of the class, news events, and/or guest speaker availability.*

	Topics/Daily Activities	Readings and Homework	Deliverable/Due Dates
		With the exception of week one, all assignments are to be completed by the start of class.	
Week 1 **1/14**	**The Threat To Communicators And Journalists** **The Privacy Dichotomoy** **The Threat Analysis Approach / Intro to Risk Analysis** **In-Class Self-Assessment: What Do I Know About My Digital Security Practices**		Discuss assignment 1: practitioner interview (Due 1/28)

Week 2 **1/21**	**Locking Down** Students will use class time to download a VPN, install 1.1.1.1., download SIGNAL, ProtonMail, perform Google, Dropbox, Facebook, Twitter privacy checks, turn on 2FA Threat Analysis: modeling scenarios	Click Here, Chapter 1-2 https://gizmodo.com/540-million-facebook-user-records-exposed-online-inclu-1833782439 https://gizmodo.com/why-ji32k7au4a83-is-a-remarkably-common-password-1833045282 https://arstechnica.com/information-technology/2012/08/passwords-under-assault/	[**Martin Luther King Day:** Monday, January 20]
Week 3 **1/28**	**The Internet Was Built To Be Weak** How networks work, http v. https, IP addresses, DNS, VPNs, TOR, SS7, Browser extensions Guest Lecturer	Click Here, Chapter 3-4 https://www.jmporup.com/95-theses-of-cyber.html	Assignment 1: (Practitioner Interview) Due
Week 4 **2/4**	**The Internet (II)** Understanding the encryption wars, device identifiers, the seven layers of the Internet, the dark web v. the open web, how apps interact with each other. Wireshark Demonstration In Class	*James Risen*, My Life As a New York Times Reporter in the Shadow of the War on Terrorism, The Intercept Slack Security Concerns Some CEOs, CNBC, 3/26/2019 Why Your Phone Is listening And Why It's Not Paranoia, *Vice* *So You Want To Be a Dark Net Drug Lord* Number One Paid App in AppStore Sends Data To China	Assignment 2: - Students should download a free PGP and TOR access node and begin to play with them. Send a message to your instructor using PGP. - Create a Github Communications landing page - Select one privacy policy for a favorite, often-used app and annotate it

		Reading about PGP and TEMPEST and encryption wars of the 1990s	
Week 5 **2/11**	**SECURE COMMUNICATION** (The life-point approach) Content v. metadata (in class demonstration), legal orders, SMS, phone calls, postal mail, SIGNAL, WhatsApp, SecureDrop; drive storage The fine print of privacy policies, and what it means in plain English	Reading: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ https://www.buzzfeednews.com/article/nicolenguyen/grindr-location-data-exposed Will Bots Break The Internet? Other reading TBD:	Assignment III due ij class
Week 6 **2/18**	**The Adversary** What governments here and abroad can do, deep packet inspection, hacking, private corporations, USC. Tokens, authentication and permission.	TBD Google Location Tracking By The Police, New York Times interactive, 4/13/2019 Mass misconfiguration exposes 13500, Naked Security, 4/03/2019 Snowden document excerpts / CIA Vault7 excerpts Bounty hunters	**Begin Assignment III**: Reverse engineer an indictment to look for tradecraft and communication lapses https://www.justice.gov/opa/press-release/file/1207916/download and https://www.justice.gov/usao-sdny/press-release/file/1101511/download

		Ronan Farrow NYer article	
Week 7 **2/25**	**The Sony Hack** **In class guest TBD:** **QUIZ based on reading and lectures**	Reading TBD	
Week 8 **3/3**	**The Border Scenario**: How to lock down your devices; device back-ups and encryption; legal rights at the border; what to do if you're detained; what to do if you're detained by LE anywhere; how to wipe clean a device. Review security basics in class.	Click Here, Chapter 7 Follow-up and restoring and backing up your devices every time you cross a border Travel only Gmail account: a practical proposal for digital privacy at the US border YouTube video on your rights	Assignment III due in class
Week 9 **3/10**	**Midterm Practicium:** "Lock Down" – help a fellow student in the Media Center secure his or her computer. Explain to them how VPNsFInal Draf, password managers, 2FA, etc. work. We will schedule students in blocks of time.	(No Reading)	**Begin Assignment IV**: Find a spot at the USC Village that you believe is safe from surveillance
Spring Break **3/17**	**NO CLASS**		
Week 10 **3/24**	**Surveillance and Sources (1):** Intro to surveillance; visit USC Village; explain next week's game	Click Here, Chapter 8	Assignment IV Due / Assessed in class

Week 11 **3/31**	**Surveillance game**	Practice surveillance and counter-surveillance!	
Week 12 **4/7**	**Surveillance hotwash** **The law: what you need to know**	Click Here, Chapter 10	**Begin: Assignment V**: Doxx your instructor for the purposes of a social engineer attack.
Week 13 **4/14**	**Doxxing, Harrassment and Mental Health online**	Reading TBD	Assignment V Due in class
Week 14 **4/21**	**New Technologies and Trust; AI, DeepFakes, Blockchain, etc.**	Reading TBD	Begin Assignment VI The Burner Phone Problem
Week 15 **4/28**	**Review course and final exam expectations**	(No Reading)	Assignment VI Due In Class
Final Exam Period **5/12, 8-10 a.m.**	Final Examination In Class		

XI. Policies and Procedures

Internships

The value of professional internships as part of the overall educational experience of our students has long been recognized by the School of Journalism. Accordingly, while internships are not required for successful completion of this course, any student enrolled in this course that undertakes and completes an approved, non-paid internship during this semester shall earn academic extra credit herein of an amount equal to 1 percent of the total available semester points for this course. To receive instructor approval, a student must request an internship letter from the Annenberg Career Development Office and bring it to the instructor to sign by the end of the third week of classes. The student must submit the signed letter to the media organization, along with the evaluation form provided by the Career Development Office. The form should be filled out by the intern supervisor and returned to the instructor at the end of the semester. No credit will be given if an evaluation form is not turned into the instructor by the last day of class. Note: The internship must by unpaid and can only be applied to one journalism or public relations class.

Statement on Academic Conduct and Support Systems

a. Academic Conduct

Plagiarism

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

USC School of Journalism Policy on Academic Integrity

The following is the USC Annenberg School of Journalism's policy on academic integrity and repeated in the syllabus for every course in the school:

"Since its founding, the USC School of Journalism has maintained a commitment to the highest standards of ethical conduct and academic excellence. Any student found plagiarizing, fabricating, cheating on examinations, and/or purchasing papers or other assignments faces sanctions ranging from an 'F' on the assignment to dismissal from the School of Journalism. All academic integrity violations will be reported to the office of Student Judicial Affairs & Community Standards (SJACS), as per university policy, as well as journalism school administrators."

In addition, it is assumed that the work you submit for this course is work you have produced entirely by yourself, and has not been previously produced by you for submission in another course or Learning Lab, without approval of the instructor.

b. Support Systems

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention and Services (RSVP) - (213) 740-9355(WELL), press "0" after hours – 24/7 on call
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office of Equity and Diversity (OED)- (213) 740-5086 | Title IX – (213) 821-8298
equity.usc.edu, titleix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants. The university prohibits discrimination or harassment based on the following *protected characteristics*: race, color, national origin, ancestry, religion, sex, gender, gender identity, gender expression, sexual orientation, age, physical disability, medical condition, mental disability, marital status, pregnancy, veteran status, genetic information, and any other characteristic which may be specified in applicable laws and governmental regulations. The university also prohibits sexual assault, non-consensual sexual contact, sexual misconduct, intimate partner violence, stalking, malicious dissuasion, retaliation, and violation of interim measures.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office of Equity and Diversity |Title IX for appropriate investigation, supportive measures, and response.

The Office of Disability Services and Programs - (213) 740-0776
dsp.usc.edu
Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

USC Support and Advocacy - (213) 821-4710
uscsa.usc.edu

Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity at USC - (213) 740-2101
diversity.usc.edu
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call
dps.usc.edu
Non-emergency assistance or information.

Annenberg Student Success Fund
https://annenberg.usc.edu/current-students/resources/additional-funding-resources
The Annenberg Student Success Fund is a donor-funded financial aid account available to USC Annenberg undergraduate and graduate students for non-tuition expenses related to extra- and co-curricular programs and opportunities.

Breaking Bread Program [undergraduate students only]
https://undergrad.usc.edu/faculty/bread/
The Breaking Bread Program is designed to provide individual undergraduate students with an opportunity to meet and have scholarly discussions with faculty members outside of the normal classroom setting. Through this program, students and faculty enjoy good company and great conversation by literally "breaking bread" over a meal together and USC will pick up the tab! Your meal event can take place anywhere outside of the normal classroom setting. Your venue can be a restaurant or eatery on or off-campus.

XII. About Your Instructors

Marc Ambinder is the author of The Brink and several other books on national security. For 20 years, he has covered politics, policy, the intelligence community, and national security. In Washington, he was a White House correspondent and a politics editor for the Atlantic.

Joshua Campbell retired in 2018 after serving for 12 years as a special agent of the Federal Bureau of Investigation. He conducted national security and criminal investigations and was a Special Assistant to former FBI Director James Comey. He is now a journalist with CNN, a term member of the Council on Foreign Relations, and a U.S. Navy Reservist.