APPLICATION FOR NOMINATION TO THE SEVENTH JUDICIAL CIRCUIT COURT

Ann M. Phillips

January 8, 2024

APPLICATION FOR NOMINATION TO THE SEVENTH JUDICIAL CIRCUIT COURT

Instructions: *Respond fully to the questions asked below. Please make all efforts to include your full answer to each question in this document. You may attach additional pages, as necessary, however it is discouraged. In addition to the application, you must provide a recent color photograph to help identify yourself.*

Full Name: Ann Muenzmay Phillips **Social Security No.:** [redacted]

Florida Bar No.: 978698 **Date Admitted to Practice in Florida:** 7/23/1993

1. Please state your current employer and title, including any professional position and any public or judicial office you hold, your business address and telephone number.

   Embry-Riddle Aeronautical University
   Associate Professor of Homeland Security & Intelligence
   Security Studies & International Affairs Department
   1 Aerospace Boulevard
   Daytona Beach, Florida 32114
   386-226-2966

2. Please state your current residential address, including city, county, and zip code. Indicate how long you have resided at this location and how long you have lived in Florida. Additionally, please provide a telephone number where you can be reached (preferably a cell phone number), and your preferred email address.

   [redacted]
   I have resided at this address since March 2000.
   I have lived in Florida my entire life.
   I can be reached on my cell phone at [redacted]
   My preferred email address is amphil1227@gmail.com

3. State your birthdate and place of birth.

   June 20, 1966
   Sarasota, Florida

4. Are you a registered voter in Florida (Y/N)?

   Yes

5. Please list all courts (including state bar admissions) and administrative bodies having special admissions requirements to which you have ever been admitted to practice, giving the dates of

admission, and if applicable, state whether you have ever been suspended or resigned. Please explain the reason for any lapse in membership.

- The Florida Bar (1993 – present)
- United States Supreme Court (2003 – present)
- United States Court of Appeals for the Eleventh Circuit (1995 – 2016) I allowed my membership to lapse as I no longer appear before this court.
- United States District Court, Middle District of Florida (1995 – 2016). I allowed my membership to lapse as I no longer appear before this court.

6. Have you ever been known by any aliases? If so, please indicate and when you were known by such alias.

   Birth – August 1990 - Ann Muenzmay
   August 1990 - December 1997 - Ann Muenzmay Childs
   December 1997 - present – Ann Muenzmay Phillips

EDUCATION:

7. List in reverse chronological order each secondary school, college, university, law school or any other institution of higher education attended and indicate for each the dates of attendance, whether a degree was received, the date the degree was received, class standing, and graduating GPA (if your class standing or graduating GPA is unknown, please request the same from such school).

   - University of Florida
     - January 1990 – December 1992
     - Degree earned: Juris Doctor
     - Date received: December 19, 1992
     - Graduating GPA: 2.8
   - University of South Florida
     - August 1984 – December 1987
     - Degree earned: Bachelor of Arts, Political Science
     - Date received: December 13, 1987
     - Graduating GPA: 3.1
   - Sarasota High School
     - August 1980 - June 1984
     - Degree earned: High School diploma
     - Date received: June 7, 1984
     - Graduating GPA: 3.8

8. List and describe any organizations, clubs, fraternities or sororities, and extracurricular activities you engaged in during your higher education. For each, list any positions or titles you held and the dates of participation.

   - University of Florida
     - Guardian Ad Litem volunteer, 1991-1993

- Chapter Advisor, Alpha Omicron Pi, 1990-1993
- John Marshall Bar Association, 1990-1992

- University of South Florida
  - Student Government, Senator, College of Social & Behavioral Sciences, 1986-1987
    - Budget Committee member
  - Young Republicans, 1985-1987
  - Alpha Omicron Pi Fraternity, collegiate member, 1985-1987
    - Vice-President of Recruitment, 1985-1986
    - Keeper of the Ritual, 1986-1987
    - Panhellenic Representative, 1986-1987
  - Order of Omega, Honor Society, 1986-1987
    - Secretary, 1987
  - Senior Class Council, 1987

EMPLOYMENT:

9. List in reverse chronological order all full-time jobs or employment (including internships and clerkships) you have held since the age of 21. Include the name and address of the employer, job title(s) and dates of employment. For non-legal employment, please briefly describe the position and provide a business address and telephone number.

Embry-Riddle Aeronautical University, Daytona Beach (August 2015 – present)
Associate Department Chair, Security Studies & International Affairs (August 2023 – present)
Associate Professor of Homeland Security & Intelligence (August 2021 – present)
Program Coordinator, Homeland Security & Intelligence (August 2018 – August 2023)
Assistant Professor of Homeland Security (August 2015 – August 2021)
Security Studies & International Affairs Department
1 Aerospace Blvd.
Daytona Beach, Florida 32114
386-226-7517

- I am a full-time associate professor teaching various courses, primarily in legal studies and cybersecurity. In 2019, I was promoted by an interdisciplinary committee to associate professor from assistant professor, the same year I was first eligible for this promotion. I served as the program coordinator for the Homeland Security & Intelligence degree program, overseeing faculty members, students, administrative requirements, and budgeting. In August 2023, I was named the associate department chair. I am continuing with similar oversight duties, which have been expanded to include the department's other degree program, Global Conflict Studies, and its faculty.

Aaron Delgado & Associates
Contract appellate attorney (2022 – present)
227 Seabreeze Blvd.
Daytona Beach, Florida 32118

Embry-Riddle Aeronautical University, Worldwide Campus
Course Developer and Adjunct Faculty (May 2016 – May 2019)
1 Aerospace Blvd.
Daytona Beach, Florida 32114
800-522-6787

College of Arts & Sciences, Security & Emergency Services

- Developed course curriculum for graduate and undergraduate online delivery (two graduate/two undergraduate): International Law and U.S. Security Policy, Aviation Policy and Law in Cyberspace, Homeland Security Law and Policy, and Cybercrime and Cyberlaw.
- Provided online graduate and undergraduate instruction in courses I created.

State of Florida, Department of Legal Affairs, Office of the Attorney General
Assistant Attorney General, Criminal Division (February 1994 – May 2015)
444 Seabreeze Blvd.
Suite 500
Daytona Beach, Florida 32118

Embry-Riddle Aeronautical University
Adjunct Professor, College of Arts and Sciences (August 2013 – August 2015)
1 Aerospace Blvd.
Daytona Beach, Florida 32114
386-226-7517

- I taught one Homeland Security Law & Policy class each semester for the Homeland Security program.

Embry-Riddle Aeronautical University
Adjunct Professor, College of Business (August 1996 – May 1999)
1 Aerospace Blvd.
Daytona Beach, Florida 32114
386-226-6100

- I taught one Business Law class for the College of Business each semester.

Dickinson & Gibbons, P.A.
Legal Intern (March 1993 – February 1994)
401 N. Cattleman Rd.
Suite 300
Sarasota, Florida 34232

- Provided support in a general civil litigation and appellate practice firm.

Department of Justice, United States Attorney General, Northern District of Florida
Legal Intern (August 1992 – December 1992)
United States Courthouse
401 S.E. 1st Ave.
Gainesville, Florida 32601

- Provided support primarily in the criminal division with some civil litigation.

Clayton, Johnston, Quincey, Ireland, Felder, Gadd, Smith & Roundtree, P.A.
Legal Intern (January 1991 – August 1994)
111 S.E. 1st Ave.
Gainesville, Florida 32601

- Provided support in general civil practice firm.

10. Describe the general nature of your current practice including any certifications which you possess; additionally, if your practice is substantially different from your prior practice or if you are not now practicing law, give details of prior practice. Describe your typical clients or former clients and the problems for which they sought your services.

I achieved board certification in Criminal Appellate law in August 1999 and have remained certified since then. My current certification period ends in 2024.

Prior to my employment with Embry-Riddle Aeronautical University, I was an Assistant Attorney General for the State of Florida. In that capacity, I handled felony criminal appeals for all the circuits within the jurisdiction of Florida's Fifth District Court of Appeal. My practice consisted of all aspects of criminal appellate law in state and federal courts. I handled appeals in felony cases, including all levels of homicides (excluding death penalty cases), assault and battery, stalking, kidnapping & false imprisonment, sex offenses (including capital sexual battery), robbery, burglary, fraud, and child abuse. I would be solely responsible for the cases assigned to me and would address all issues raised in the opponents' briefs. Typical issues raised on appeal would include a review of state constitutional issues, statutory challenges, United States constitutional claims under the Fourth, Fifth, Sixth, and Eighth Amendments, evidentiary claims of error, jury selection issues, sentencing errors, and claims of prosecutorial error. I also handled petitions for post-conviction relief and claims of ineffective assistance of both trial and appellate counsel. Claims of statutory and constitutional construction and interpretation were commonplace, as were claims of various procedural errors. In addition to standard appellate briefs, I responded to all extraordinary writs, such as mandamus, certiorari, and habeas corpus, including federal petitions for habeas corpus.

11. What percentage of your appearance in court in the last five years or in the last five years of practice (include the dates) was:

Court		Area of Practice	
Federal Appellate	_____ %	Civil	_____ %
Federal Trial	_____ %	Criminal	90 %
Federal Other	10 %	Family	_____ %
State Appellate	90 %	Probate	_____ %
State Trial	_____ %	Other	10 %
State Administrative	_____ %		
State Other	_____ %		
TOTAL	100 %	TOTAL	100 %

If your appearance in court the last five years is substantially different from your prior practice, please provide a brief explanation:

Since I have been teaching for more than five years, I have not appeared in court. While at the Attorney General's Office, I appeared in multiple courts as set forth in this application.

12. In your lifetime, how many (number) of the cases that you tried to verdict, judgment, or final decision were:

Jury?	0	Non-jury?	5
Arbitration?	0	Administrative Bodies?	0
Appellate?	Thousands		

13. Please list every case that you have argued (or substantially participated) in front of the United States Supreme Court, a United States Circuit Court, the Florida Supreme Court, or a Florida District Court of Appeal, providing the case name, jurisdiction, case number, date of argument, and the name(s), e-mail address(es), and telephone number(s) for opposing appellate counsel. If there is a published opinion, please also include that citation.

Being employed by the Florida Attorney General's Office provided me with the unique experience of handling thousands of cases in the Florida appellate courts and hundreds of cases in the federal court system. A search of the Attorney General's Office files indicates more than 4,000 cases in which I was the counsel of record. I was the sole or primary attorney for most of those cases. A

smaller percentage of those cases would have involved only *pro forma* responses and did not include legal research and writing on my part.

I have handled cases at every level of the state and federal court systems. I have filed pleadings in state trial courts, multiple Florida District Courts of Appeal, the Florida Supreme Court, federal district courts, and the federal appellate court.

United States Court of Appeals for the Eleventh Circuit

I was counsel of record in approximately a dozen cases. I presented oral argument in one case.

Thompson v. Secretary, Department of Corrections, 595 F.3d 1233 (11th Cir. 2010)
Oral argument on September 21, 2009
Opposing Counsel: Appointed Counsel for Appellant, Elaine Joan Mittleman, elainemittleman@msn.com, (703) 734-0482

Florida Supreme Court

I was counsel of record in more than thirty cases and appeared for oral argument in the following matters:

Andre Isaiah Dunbar v. State of Florida, 89 So. 3d 901 (Fla. 2012)
Oral argument on November 2, 2011
Opposing counsel: Assistant Public Defender David Stewart Morgan, morgan.dave@pd7.org, (386) 689-8857

State of Florida v. Tony A. Carwise, 846 So. 2d 1145 (Fla. 2003)
Oral argument on March 3, 2003
Opposing counsel: Leonard R. Ross, lrr@fldivorcesite.com, (386) 258-5069 and George D.E. Burden, georgeburdenlaw@gmail.com, (386) 451-6968

Fifth District Court of Appeal

I was counsel of record in more than one thousand cases in the Fifth District Court of Appeal. I would estimate that I appeared for oral argument approximately fifty times. If desired, a list of cases could be generated.

14. Within the last ten years, have you ever been formally reprimanded, sanctioned, demoted, disciplined, placed on probation, suspended, or terminated by an employer or tribunal before which you have appeared? If so, please state the circumstances under which such action was taken, the date(s) such action was taken, the name(s) of any persons who took such action, and the background and resolution of such action.

No.

15. In the last ten years, have you failed to meet any deadline imposed by court order or received notice that you have not complied with substantive requirements of any business or contractual arrangement? If so, please explain full.

No.

16. For your last six cases, which were tried to verdict or handled on appeal, either before a jury, judge, appellate panel, arbitration panel or any other administrative hearing officer, list the names, e-mail addresses, and telephone numbers of the trial/appellate counsel on all sides and court case numbers (include appellate cases). *This question is optional for sitting judges who have served five years or more.*

A) *Noah Dickerhoff v. State of Florida*, 5D21-2594
Richard Pallas, Counsel for Appellee
Richard.pallas@myfloridalegal.com
(386) 238-4990

B) *Robert Lentino v. Torianne McKinney*, 5D21-2155
No appearance by Appellee

C) *Alexey Kholodkov v. State of Florida*, 5D15-665
Ronald E. Fox, Counsel for Appellant
ron@ronfoxlawyer.com
(352) 669-3228

D) *Michael P. Matos v. State of Florida*, 5D14-2704
Michael Matos, *pro se* Appellant

E) *Michael P. Matos v. State of Florida*, 5D14-4428
Michael Matos, *pro se* Appellant

F) *Kenneth Earl Jackson v. State of Florida*, 5D14-1400
William R. Ponall, Counsel for Appellant
bponall@ponalllaw.com
(407) 622-1144

17. For your last six cases, which were either settled in mediation or settled without mediation or trial, list the names and telephone numbers of trial counsel on all sides and court case numbers (include appellate cases). *This question is optional for sitting judges who have served five years or more.*

Not applicable.

18. During the last five years, on average, how many times per month have you appeared in Court or at administrative hearings? If during any period you have appeared in court with greater frequency than during the last five years, indicate the period during which you appeared with greater frequency and succinctly explain.

I have not appeared in court in the past five years as I have been primarily employed as a university professor during the stated period.

When employed at the Florida Attorney General's Office, I appeared as appellate counsel in those cases set for oral argument which included my cases before the Fifth District Court of Appeal, the Florida Supreme Court, the Middle District of Florida, the Eleventh Circuit Court of Appeals, and several circuit courts. I also appeared in evidentiary hearings, depositions, and various motion hearings in both state and federal trial courts.

During my time of employment, during the early 2000s, I also assisted in representing the Florida Department of Highway Safety and Motor Vehicles in civil forfeitures in the circuit court. My participation included handling preliminary probable cause hearings, status hearings, pretrial conferences, hearings on motions to dismiss, and motions for summary judgments.

19. If Questions 16, 17, and 18 do not apply to your practice, please list your last six major transactions or other legal matters that were resolved, listing the names, e-mail addresses, and telephone numbers of the other party counsel.

Not applicable.

20. During the last five years, if your practice was greater than 50% personal injury, workers' compensation or professional malpractice, what percentage of your work was in representation of plaintiffs or defendants?

Not applicable.

21. List and describe the five most significant cases that you personally litigated giving the case style, number, court and judge, the date of the case, the names, e-mail addresses, and telephone numbers of the other attorneys involved, and citation to reported decisions, if any. Identify your client and describe the nature of your participation in the case and the reason you believe it to be significant.

- *State v. Traylor*, 77 So. 3d 224 (Fla. 5th DCA 2011) (5D10-1301)
    - Judges: Richard B. Orfinger, Jacqueline R. Griffin, and Jay P. Cohen
    - Opposing counsel: Bradley S. Sherman, bradleystu@msn.com, 386-453-0500
    - This opinion was based on the State's appeal from an order quashing several charges against the Appellees. The Office of Statewide Prosecution had charged the Appellees with multiple counts regarding a "down payment assistance" program they had operated. The scheme had lasted several years, many counts were charged, and the charging information had been amended. After a jury trial, a judgment of acquittal was granted on several charges, and a mistrial was declared on the remaining charges. The State amended the information prior to the new trial adding, *inter alia*, alleged violations of a new statute not involved in the prior information. The trial court granted the Appellees' motion to quash multiple counts. The Fifth District Court of Appeal found that while the trial court had properly dismissed counts barred by the statute of limitations, the aggravated white-collar crime had been improperly dismissed. In analyzing the case, the court looked at the specific language of the statute Appellees allegedly violated, the dates of the offenses, and the dates of the amendments in order to determine whether the charge was timely. This case is significant in that it interpreted the specific language of the statute in conjunction with the dates of the offenses to demonstrate interpretation of the statute of limitations in cases with multiple counts and multiple informations over multiple years.
- *McKinney v. State*, 66 So. 3d 852 (Fla. 2011) (SC10-140)
    - Justices: Charles T. Canady, Barbara J. Pariente, Ricky Polston, Jorge Labarga, James E.C. Perry, R. Fred Lewis, Peggy A. Quince
    - Opposing counsel: Rebecca M. Becker, rmbmsb@outlook.com, 386-672-6092
    - The Florida Supreme Court resolved a conflict regarding double jeopardy between the Fifth and Fourth District Courts of Appeal. McKinney had been charged with grand theft and robbery with a firearm from a single criminal episode. The Supreme Court approved the opinion of the Fifth District Court of Appeal. The Florida Supreme Court applied its recent line of reasoning in *Valdes v. State*, 3 So. 3d 1067 (Fla. 2009), which receded from its prior interpretation for discerning double jeopardy violations. I wrote the brief for the case in the district court as well.
- *State v. Oliveras*, 65 So. 3d 1162 (Fla. 5th DCA 2011) (5D09-4197)
    - Judges: Thomas D. Sawaya, Richard B. Orfinger, and Bruce W. Jacobus
    - Opposing counsel: Kathryn Radtke, radtke.kathryn@pd7.org, 386-254-3758
    - In this state appeal, the court interpreted Florida's Security of Communications Act as it related to a computer tracing company's tracing of the victim's computer and whether this constituted a violation of the defendant's Fourth Amendment rights. The court

found that since there was no state action and the tracing company was acting at the request of the person who had paid for their services, Oliveras had no reasonable expectation of privacy under the Fourth Amendment.

- *Freeman v. State*, 969 So. 2d 473 (Fla. 5th DCA 2007) (5D06-2395)
    - Judges: Robert J. Pleus, Jr., William D. Palmer, and Alan Lawson
    - Opposing counsel: Brynn Newton (retired), thenewcons@aol.com, 386-846-2428
    - This case struck a chord with me as the victim's family was genuinely concerned about the appeal of the defendant's manslaughter conviction. The case was interesting from a legal perspective as it highlighted the charging discretion of the State Attorney, and the application of general versus specific intent crimes.
- *Barber v. State*, 781 So. 2d 425 (Fla. 5th DCA 2001) (5D99-218)
    - Judges: Earle W. Peterson, Jr., Winifred Sharp, and Robert J. Pleus, Jr.
    - Opposing counsel: Robert Berry, robert@attorneyrobertberry.com, 850-597-8015 and Gregory Eisenmenger, gregeisenmenger@ebplaw.com, 321-504-0321
    - This was a circumstantial evidence case involving aggravated child abuse, specifically shaken baby syndrome. A feature of the case was *Williams* rule (similar fact) evidence, upon which the prosecution relied to prove the defendant's identity. Barber, a church daycare provider, had been entrusted with the care of multiple infants. Two infants in Barber's care received strikingly similar injuries within a similar time frame. The injuries of the second child were presented at the trial.

22. Attach at least two, but no more than three, examples of legal writing which you personally wrote. If you have not personally written any legal documents recently, you may attach a writing sample for which you had substantial responsibility. Please describe your degree of involvement in preparing the writing you attached.

I have attached two writing samples. The first is an initial brief filed in the Fifth District Court of Appeal on behalf of Appellant Robert Lentino in Lentino v. McKinney, 5D21-2155. The second is an answer brief filed on behalf of the Appellee, the State of Florida, in Melody Daniels v. State, 5D14-0599. I was solely responsible for producing both documents.

PRIOR JUDICIAL EXPERIENCE OR PUBLIC OFFICE

23. Have you ever held judicial office or been a candidate for judicial office? If so, state the court(s) involved, the dates of service or dates of candidacy, and any election results.

No.

24. If you have previously submitted a questionnaire or application to this or any other judicial nominating commission, please give the name(s) of the commission, the approximate date(s) of each submission, and indicate if your name was certified to the Governor's Office for consideration.

Seventh Circuit JNC, County Court Vacancy, September 2023, certified
Seventh Circuit JNC, Circuit Vacancy, January 2023, certified

25. List any prior quasi-judicial service, including the agency or entity, dates of service, position(s) held, and a brief description of the issues you heard.

Not applicable.

26. If you have prior judicial or quasi-judicial experience, please list the following information:

(i) the names, phone numbers and addresses of six attorneys who appeared before you on matters of substance;
(ii) the approximate number and nature of the cases you handled during your tenure;
(iii) the citations of any published opinions; and
(iv) descriptions of the five most significant cases you have tried or heard, identifying the citation or style, attorneys involved, dates of the case, and the reason you believe these cases to be significant.

Not applicable.

27. Provide citations and a brief summary of all of your orders or opinions where your decision was reversed by a reviewing court or where your judgment was affirmed with significant criticism of your substantive or procedural rulings. If any of the opinions listed were not officially reported, attach copies of the opinions.

Not applicable.

28. Provide citations for significant opinions on federal or state constitutional issues, together with the citation to appellate court rulings on such opinions. If any of the opinions listed were not officially reported, attach copies of the opinions.

Not applicable.

29. Has a complaint about you ever been made to the Judicial Qualifications Commission? If so, give the date, describe the complaint, whether or not there was a finding of probable cause, whether or not you have appeared before the Commission, and its resolution.

Not applicable.

30. Have you ever held an attorney in contempt? If so, for each instance state the name of the attorney, case style for the matter in question, approximate date and describe the circumstances.

Not applicable.

31. Have you ever held or been a candidate for any other public office? If so, state the office, location, dates of service or candidacy, and any election results.

Not applicable.

NON-LEGAL BUSINESS INVOLVEMENT

32. If you are now an officer, director, or otherwise engaged in the management of any business enterprise, state the name of such enterprise, the nature of the business, the nature of your duties, and whether you intend to resign such position immediately upon your appointment or election to judicial office.

I am not engaged in any for-profit business, but I am a director on a not-for-profit board.

I currently serve as a member of the Board of Trustees for Daytona Beach's Museum of Arts and Sciences. MOAS is a not-for-profit educational institution, the mission of which is to inspire, cultivate curiosity, and promote lifelong learning in art, science, and history. I currently serve as the Secretary, Collections Committee Chair, and the Nominating Committee Chair. I am enthusiastic about the contributions MOAS brings to this community and the State of Florida but would seek to stay on the board in an appropriate capacity without fundraising but would resign in the should it become prudent.

33. Since being admitted to the Bar, have you ever engaged in any occupation, business or profession other than the practice of law? If so, explain and provide dates. If you received any compensation of any kind outside the practice of law during this time, please list the amount of compensation received.

In the late 1990s and into the early 2000s, and again in 2012-2014, I taught as an adjunct faculty for Embry-Riddle Aeronautical University. I taught Business Law and Homeland Security Law & Policy as an adjunct. As an adjunct, I received $3,000 per course.

I became a full-time professor at ERAU in 2015 and remain employed in that capacity. I teach courses in Homeland Security Law & Policy, Government of the U.S., and Cybercrime & Cyberlaw. As a full-time employee, I have received a regular salary, the details of which are set forth more fully in the financial disclosure. My compensation for the most recent calendar year, 2023, was approximately $98,000.

POSSIBLE BIAS OR PREJUDICE

34. The Commission is interested in knowing if there are certain types of cases, groups of entities, or extended relationships or associations which would limit the cases for which you could sit as the presiding judge. Please list all types or classifications of cases or litigants for which you, as a general proposition, believe it would be difficult for you to sit as the presiding judge. Indicate the reason for each situation as to why you believe you might be in conflict. If you have prior judicial experience, describe the types of cases from which you have recused yourself.

No, I do not believe that there are any general groups, relationships, or associations that would limit the cases for which I could sit as the presiding judge. Neither are the classifications of cases or litigants for which I would find it difficult to sit as the presiding judge.

PROFESSIONAL ACCOMPLISHMENTS AND OTHER ACTIVITIES

35. List the titles, publishers, and dates of any books, articles, reports, letters to the editor, editorial pieces, or other published materials you have written or edited, including materials published only on the Internet. Attach a copy of each listed or provide a URL at which a copy can be accessed.

- Phillips, A.M., "Foreign Intelligence Surveillance Act of 1978," J. Rudolph & W. Lahneman (Eds.) *Combatting Terrorism in the 21st Century: American Laws, Strategies and Agencies.* Santa Barbara, CA. ABC-CLIO.

- Phillips, A.M., "Foreign Intelligence Surveillance Court," J. Rudolph & W. Lahneman (Eds.) *Combatting Terrorism in the 21st Century: American Laws, Strategies and Agencies.* Santa Barbara, CA. ABC-CLIO.

- Kessler, G.C. and Phillips, A.M. (August 2020) "Cryptography, Passwords, Privacy, and the Fifth Amendment," Journal of Digital Forensics, Security and Law.

A copy of each article is attached. Please note that for the journal article that I co-authored with Dr. Gary Kessler, I cannot claim any credit for the portion of the article that addresses the history of cryptography; Section 2 is solely Dr. Kessler's work. My contributions are reflected in the legal aspects of the article.

36. List any reports, memoranda or policy statements you prepared or contributed to the preparation of on behalf of any bar association, committee, conference, or organization of which you were or are a member. Provide the name of the entity, the date published, and a summary of the document. To the extent you have the document, please attach a copy or provide a URL at which a copy can be accessed.

Not applicable.

37. List any speeches or talks you have delivered, including commencement speeches, remarks, interviews, lectures, panel discussions, conferences, political speeches, and question-and-answer sessions. Include the date and place they were delivered, the sponsor of the presentation, and a summary of the presentation. If there are any readily available press reports, a transcript or recording, please attach a copy or provide a URL at which a copy can be accessed.

- Sharp, M., Berezovski, M., Gressang, D., Phillips, A., et al. *Media Literacy and Online Critical Thinking Initiatives*, Seminar for Volusia County Schools (May 2023, June 2023). https://commons.erau.edu/faculty-research-projects/37/ (part of DHS TVTP grant)
- Phillips, A.M. Homeland Security Law & Policy. 2023 ERAU Aviation Regulation in the U.S. Law Seminar, April 7, 2023, Embry-Riddle Aeronautical University.
- Phillips, A.M. Cybersecurity and the Law. 2022 ERAU U.S. Aviation Law Professional Development Workshop, November 29, 2022, Embry-Riddle Aeronautical University.
- Phillips, A.M. Homeland Security Law & Policy. 2022 ERAU Aviation Regulation in the U.S. Law Seminar, April 7, 2022, Embry-Riddle Aeronautical University.
- Phillips, A.M. Cybersecurity and the Law. 2021 ERAU U.S. Aviation Law Professional Development Workshop, December 9, 2021, Embry-Riddle Aeronautical University.
- Phillips, A.M. Homeland Security Law & Policy. 2021 ERAU Aviation Regulation in the U.S. Law Seminar, April 8, 2021, Embry-Riddle Aeronautical University.
- Zorri, D.M. and Phillips, A.M., "Quantifying Risk as a Method of Reasoning Protecting Privacy at the Border." 2020 Citadel Intelligence Ethics Conference, Charleston, SC, February 11, 2020.
- Phillips, A.M. Cybersecurity and the Law. 2019 *ERAU U.S. Aviation Law Professional Development Workshop*, December 5, 2019. Embry-Riddle Aeronautical University.
- Phillips, A.M., Trends in Homeland Security. *2019 Aviation Regulation in the United States*, Part of the U.S. Aviation Law Diploma. April 11, 2019. Embry-Riddle Aeronautical University.
- Phillips, A.M., Cybersecurity Law and Policy. *2018 ERAU Aviation Law Professional Development Workshop*. December 6, 2018. Embry-Riddle Aeronautical University.
- Friedenzohn, D. and Phillips, A.M., "Constitutional Considerations and Evolving Drone Technology." Ninth Annual Constitutional Law Colloquium, Loyola University Chicago School of Law, Chicago, IL, November 3, 2018.
- Phillips, A.M., Trends in Homeland Security Law & Policy. *2018 Aviation Regulation in the United States*, Part of the U.S. Aviation Law Diploma. April 5, 2018. Embry-Riddle Aeronautical University.
- Phillips A.M., Cybersecurity Law and Policy. *2017 ERAU Aviation Law Professional Development Workshop*. December 7, 2017. Embry-Riddle Aeronautical University.
- Phillips, A.M., Cybersecurity in Aviation. *2016 ERAU U.S. Aviation Law Seminar*, December 6, 2016. Embry-Riddle Aeronautical University.

I have either presented or substantially led Embry-Riddle's Constitution Day events since 2016. I have spoken individually, led panel discussions, hosted a Constitution trivia contest, and have moderated question and answer sessions.

During my employment at the Attorney General's office, I spoke numerous times as part of the Child Predator Cyber Crime Unit's initiative to educate middle and high school students on the dangers that exist on the internet. I also spoke numerous times as the president of the Volusia Flagler Association for Women Lawyers and the Dunn-Blount American Inn of Court.

I have guest-lectured in numerous law, appeals, and legal writing classes. I have participated in many Law Week talks and presentations.

38. Have you ever taught a course at an institution of higher education or a bar association? If so, provide the course title, a description of the course subject matter, the institution at which you taught, and the dates of teaching. If you have a syllabus for each course, please provide.

All courses were taught at Embry-Riddle Aeronautical University. Master course outlines for each are attached.

BA 225 – Business Law (August 1996 – May 1999) - an overview of the law as it pertains to business relations and business transactions. Areas covered include civil procedure; torts; criminal law and procedure; constitutional law; administrative law; contracts; agency; real property; personal property; wills; trusts and estates; insurance law; employment law; commercial transactions; secured transactions; creditor/debtor law; and negotiable instruments.

CYB 465/CYBR 465 – Cybercrime & Cyberlaw (occasional offerings since 2017) - types of criminal behavior in cyberspace, such as identity theft, white collar crimes, fraud, child sexual exploitation, intellectual property theft, and online scams; laws governing cyberspace, defining criminal activity, and guiding law enforcement investigations; U.S. decisional law guiding search and seizure of digital devices and information; international laws related to computer crime and privacy.

HSI 110 – Introduction to Homeland Security (occasional offerings since 2015) - introduces the multidisciplinary approach to protecting and defending America. Knowledge domains of intelligence, emergency management, law and policy, critical infrastructure and resilience, strategic planning and decision-making, terrorism, cyberspace, human and environmental security, risk analysis and management, and professionalism.

HS 280 – Professionalism in Homeland Security (occasional offerings between 2016-2018) - prepared students to seek and win internships, personality evaluations, cover letter and resume preparation, and interviewing skills. Ethics and professionalism in homeland security.

HS 290 – Introduction to Environmental Security (occasional offerings since 2016) - Development and execution of U.S. domestic and foreign policy, transnational threats, and ultimately U.S. national security relating to emerging threats, environmental & health issues, infrastructure vulnerabilities, natural resource shortages, and urbanization in less developed countries.

HS 320/HSI 320/HSLD 320 – Homeland Security & Intelligence Law and Policy (2016 – present) - Key legal, policy, and ethical issues in the context of Homeland Security and Intelligence policy and practice; legal concepts regarding constitutional rights of individuals,

legal process, access to courts, the law of war, and national security principles as they relate to homeland security legislation and policy initiatives; legal principles of due process, habeas corpus, search and seizure, compulsory process, and international agreements are explored. Elements of national security law, including intelligence collection and sharing, the Patriot Act, and military-civilian relations.

MCMP 515/MHSR 515 – Law & Policy for National, Human, and Cyber Security (Spring 2016, Summer 2019) - examines the role of international law, U.S. foreign policy, and international institutions in responding to terrorism, crime, complex emergencies, disasters and crises; analyzes the challenges and difficulties in achieving unified response and the administrative and legal barriers that must be overcome; discusses how U.S. laws and policies intersect with international norms and regimes in a U.S. security context, including existing multinational treaties such as UNCLOS and the Antarctic Treaty System, International Cybercrime Treaty, the Biological Weapons Convention or the Chemical Weapons Convention, and international humanitarian law. Particular attention is paid to privacy law; conflicts that are caused by disparate laws and policies are also explored, as well as solutions.

MCMP 516 – Aviation Policy and Law in Cyberspace (Spring 2018) - addresses emerging policies and laws that affect cyberspace, particularly related to information security and cybercrime in the aviation and aerospace industry; the clash between real space and cyberspace is examined, as well as international laws and policies related to aviation, aerospace, and aeronautics.

SS 320/HSI 323 – Government of the U.S. (Fall 2020, Fall 2023-present) - introduces the nature of constitutional government at the national level, contributing to a greater understanding and political awareness among an informed citizenry; students are introduced to rules, institutions, and concepts to demonstrate the allocation of power and resources in political conflict, supporting an understanding that the U.S. political process inevitably involves its citizens, regardless of their involvement in politics.

39. List any fellowships, honorary degrees, academic or professional honors, honorary society memberships, military awards, and any other special recognition for outstanding service or achievement. Include the date received and the presenting entity or organization.

Impact Award – Awarded by the ERAU Daytona Beach Parent Association/Parent Advisory Council – 2023
Service Recognition – Child Predator Cyber Crime Unit – 2008, 2009, 2010
Service Recognition – Volunteer Lawyer's Project – 2000, 2008
Pro Bono Award – 2007
Service Recognition – Guardian Ad Litem -1996
Service Recognition – Greek Advisor - 1993
Service Recognition – Student Intern – 1992

I am also part of a group of professors at ERAU who were awarded a nearly $250,000 grant from the Department of Homeland Security as part of their Targeted Violence and Terrorism Prevention Program. This was a competitive grant process; we were one of thirty-seven recipients across the United States. This is the only federal grant program dedicated to enhancing the capabilities of local communities to prevent targeted violence and terrorism. The grants in this cycle prioritized the prevention of domestic violent extremism, including through efforts to counter online radicalization and mobilization to violence. We are in the second year of the two-year grant.

40. Do you have a Martindale-Hubbell rating? If so, what is it and when was it earned?

I am BV-rated. I am uncertain when the rating was earned.

41. List all bar associations, legal, and judicial-related committees of which you are or have been a member. For each, please provide dates of membership or participation. Also, for each indicate any office you have held and the dates of office.

- **The Federalist Society** (2022-present)
- **Dunn-Blount American Inn of Court** – (2014-present) (Immediate Past President, 2021-2023, President, 2019-2021; President-elect, 2017-2019; Secretary, 2015-2017; Executive Board member 2014-15, 2023-2025)
- **Volusia County Bar Association** (Director 1998-2001, Secretary 1996-1997, member 1994-2012, 2022-present)
- **Volusia Flagler Association for Women Lawyers** (2010-2016, 2022-present) (President 2014-15; Vice-President 2013-2014; Secretary 2011-2013)
- **Florida Bar** (Appellate Section, Legislative Committee 2007-2009, 2020-2022) (judge for mock appellate competition, July 2023)
- **American Bar Association**, Law School Divisions Competition, Appellate Brief grader (2020-2021)
- **Volusia County Teen Court, Development Committee** (1995-1996)
- **Volusia County Teen Court** volunteer (1996-2005)
- **Juvenile Drug Court Task Force Committee** (2002-2003)
- **Adult Drug Court Task Force Committee** (2003-2005)
- **Volusia County Young Lawyers** (1995-1999)

42. List all professional, business, fraternal, scholarly, civic, charitable, or other organizations, other than those listed in the previous question to which you belong, or to which you have belonged since graduating law school. For each, please provide dates of membership or participation and indicate any office you have held and the dates of office.

- Museum of Arts & Sciences, Board of Directors (2019-present) (Secretary, 2022-present)
- Take Stock in Children of Florida, mentor high school students, 2023-present
- Community Legal Services of Mid-Florida, volunteer, multiple years
- Lighthouse Christ Presbyterian Church, Ormond Beach, 2022-present
- Sigma Kappa Sorority, faculty advisor, 2020-present

- National Security Student Association, faculty advisor, 2018-present
- International Studies Association (2016-2020)
- Pathways Elementary PTA (President 2009-2011, 2013-2014)
- Pathways Elementary School Advisory Council (2006-2015)
- Volusia County School Advisory Council, school representative (2012-2015)
- Hinson Middle School PTSA (Vice-President 2012-2014)
- Volusia County Teacher of the Year Selection Committee (2014)
- Ormond Beach Soccer Club, Girls Team Manager (2013-2015)
- Alpha Omicron Pi Fraternity, Collegiate Network Specialist (1990-2003)
- Justice Teaching Program (2007-2009)
- Volusia County Friends of Teen Court Board (Secretary)
- Guardian Ad Litem (Family Law division)
- Junior League of Daytona Beach (1997-1999)

43. Do you now or have you ever belonged to a club or organization that in practice or policy restricts (or restricted during the time of your membership) its membership on the basis of race, religion (other than a church, synagogue, mosque or other religious institution), national origin, or sex (other than an educational institution, fraternity or sorority)? If so, state the name and nature of the club(s) or organization(s), relevant policies and practices and whether you intend to continue as a member if you are selected to serve on the bench.

I was a member of the Junior League of Daytona Beach for two years in the late 1990s. The Junior League of Daytona Beach is an organization of women committed to promoting volunteering, developing the potential of women, and improving communities through the effective action and leadership of trained volunteers. Its purpose is exclusively educational and charitable. Its intent is to positively impact the communities of Volusia and Flagler Counties. This chapter is a member of the Association of Junior Leagues International, Inc. I have not been a member of the Junior League since approximately 1999.

44. Please describe any significant pro bono legal work you have done in the past 10 years, giving dates of service.

I have helped senior citizens with various scams and cyber fraud issues. No court cases have ever come from any of the incidents.

In Spring 2023, I participated in legal training with Community Legal Services to assist clients needing will and probate legal assistance. I completed one case and am currently in the process of finalizing a second case.

In addition to teaching classes, I also mentor two collegiate groups at Embry-Riddle Aeronautical University. My frequent contact with so many students often results in requests for legal counseling, which I provide. None of these situations has ever resulted in a case being filed in which I played a role.

45. Please describe any hobbies or other vocational interests.

I enjoy reading, listening to audiobooks and podcasts, cooking, watching and attending sporting events (high school, collegiate, and professional), going to the beach, going to museums, and traveling anywhere especially with my family.

46. Please state whether you have served or currently serve in the military, including your dates of service, branch, highest rank, and type of discharge.

I have never served in the military. My father served in the Army, and my husband served in the Air Force. Both were honorably discharged.

47. Please provide links to all social media and blog accounts you currently maintain, including, but not limited to, Facebook, Twitter, LinkedIn, and Instagram.

Facebook: Ann Muenzmay Phillips (https://www.facebook.com/)

Twitter: @AnnPhillips66 (https://www.twitter.com/home)

LinkedIn: Ann Phillips (https://www.linkedin.com/feed/)

Instagram: annm_phillips (https://www.instagram.com)

Pinterest: @amp5 (https://www.pinterest.com/amp5)

Snapchat: a_phillips1227 (https://www.snapchat.com/)

FAMILY BACKGROUND

48. Please state your current marital status. If you are currently married, please list your spouse's name, current occupation, including employer, and the date of the marriage. If you have ever been divorced, please state for each former spouse their name, current address, current telephone number, the date and place of the divorce and court and case number information.

I am married to John M. Phillips. We were married on December 27, 1997. He is the Athletic Director at Embry-Riddle Aeronautical University.

I was previously married to Robert Wayne Childs. Current address and telephone number are unknown. Divorced: May 25, 1993, Alachua County Circuit Court, Gainesville, Florida, Case 01-93-01514-CA.

49. If you have children, please list their names and ages. If your children are over 18 years of age, please list their current occupation, residential address, and a current telephone number.

- Lauren Elyse Phillips, 22 years of age, graduate student. Residence: 15 Noble Woods Way, Ormond Beach, Florida 32174. [redacted]

- Zachary John Phillips, 22 years of age, graduate student. Residence: 15 Noble Woods Way, Ormond Beach, Florida 32174. [redacted]
- Rachel Layne Phillips, 20 years of age, student. Residence: 15 Noble Woods Way, Ormond Beach, Florida 32174. [redacted]

CRIMINAL AND MISCELLANEOUS ACTIONS

50. Have you ever been convicted of a felony or misdemeanor, including adjudications of guilt withheld? If so, please list and provide the charges, case style, date of conviction, and terms of any sentence imposed, including whether you have completed those terms.

No.

51. Have you ever pled nolo contendere or guilty to a crime which is a felony or misdemeanor, including adjudications of guilt withheld? If so, please list and provide the charges, case style, date of conviction, and terms of any sentence imposed, including whether you have completed those terms.

No.

52. Have you ever been arrested, regardless of whether charges were filed? If so, please list and provide sufficient details surrounding the arrest, the approximate date and jurisdiction.

No.

53. Have you ever been a party to a lawsuit, either as the plaintiff, defendant, petitioner, or respondent? If so, please supply the case style, jurisdiction/county in which the lawsuit was filed, case number, your status in the case, and describe the nature and disposition of the matter.

- Case 01-93-01514-CA
  - Ann M. Childs v. Robert Wayne Childs
  - Alachua County Circuit Court
  - Petitioner
  - Final Judgment of Dissolution of Marriage, entered May 25, 1993

54. To your knowledge, has there ever been a complaint made or filed alleging malpractice as a result of action or inaction on your part?

No.

55. To the extent you are aware, have you or your professional liability carrier ever settled a claim against you for professional malpractice? If so, give particulars, including the name of the client(s), approximate dates, nature of the claims, the disposition and any amounts involved.

No.

56. Has there ever been a finding of probable cause or other citation issued against you or are you presently under investigation for a breach of ethics or unprofessional conduct by any court, administrative agency, bar association, or other professional group. If so, provide the particulars of each finding or investigation.

No.

57. To your knowledge, within the last ten years, have any of your current or former co-workers, subordinates, supervisors, customers, clients, or the like, ever filed a formal complaint or accusation of misconduct including, but not limited to, any allegations involving sexual harassment, creating a hostile work environment or conditions, or discriminatory behavior against you with any regulatory or investigatory agency or with your employer? If so, please state the date of complaint or accusation, specifics surrounding the complaint or accusation, and the resolution or disposition.

No.

58. Are you currently the subject of an investigation which could result in civil, administrative, or criminal action against you? If yes, please state the nature of the investigation, the agency conducting the investigation, and the expected completion date of the investigation.

No.

59. Have you ever filed a personal petition in bankruptcy or has a petition in bankruptcy been filed against you, this includes any corporation or business entity that you were involved with? If so, please provide the case style, case number, approximate date of disposition, and any relevant details surrounding the bankruptcy.

No.

60. In the past ten years, have you been subject to or threatened with eviction proceedings? If yes, please explain.

No.

61. Please explain whether you have complied with all legally required tax return filings. To the extent you have ever had to pay a tax penalty or a tax lien was filed against you, please explain giving the date, the amounts, disposition, and current status.

Yes, I have always filed my tax returns in a timely manner. No, I have never had to pay a tax penalty or had a tax lien filed against me.

HEALTH

62. Are you currently addicted to or dependent upon the use of narcotics, drugs, or alcohol?

No.

63. During the last ten years have you been hospitalized or have you consulted a professional or have you received treatment or a diagnosis from a professional for any of the following: Kleptomania, Pathological or Compulsive Gambling, Pedophilia, Exhibitionism or Voyeurism? If your answer is yes, please direct each such professional, hospital and other facility to furnish the Chairperson of the Commission any information the Commission may request with respect to any such hospitalization, consultation, treatment or diagnosis. ["Professional" includes a Physician, Psychiatrist, Psychologist, Psychotherapist or Mental Health Counselor.] Please describe such treatment or diagnosis.

No.

64. In the past ten years have any of the following occurred to you which would interfere with your ability to work in a competent and professional manner: experiencing periods of no sleep for two or three nights, experiencing periods of hyperactivity, spending money profusely with extremely poor judgment, suffering from extreme loss of appetite, issuing checks without sufficient funds, defaulting on a loan, experiencing frequent mood swings, uncontrollable tiredness, falling asleep without warning in the middle of an activity. If yes, please explain.

No.

65. Do you currently have a physical or mental impairment which in any way limits your ability or fitness to properly exercise your duties as a member of the Judiciary in a competent and professional manner? If yes please explain the limitation or impairment and any treatment, program or counseling sought or prescribed.

No.

66. During the last ten years, have you ever been declared legally incompetent or have you or your property been placed under any guardianship, conservatorship or committee? If yes, provide full details as to court, date, and circumstances.

No.

67. During the last ten years, have you unlawfully used controlled substances, narcotic drugs, or dangerous drugs as defined by Federal or State laws? If your answer is "Yes," explain in detail. (Unlawful use includes the use of one or more drugs and/or the unlawful possession or distribution of drugs. It does not include the use of drugs taken under supervision of a licensed health care professional or other uses authorized by Federal or State law provisions.)

No.

68. In the past ten years, have you ever been reprimanded, demoted, disciplined, placed on probation, suspended, cautioned, or terminated by an employer as result of your alleged

consumption of alcohol, prescription drugs, or illegal drugs? If so, please state the circumstances under which such action was taken, the name(s) of any persons who took such action, and the background and resolution of such action.

No.

69. Have you ever refused to submit to a test to determine whether you had consumed and/or were under the influence of alcohol or drugs? If so, please state the date you were requested to submit to such a test, the type of test required, the name of the entity requesting that you submit to the test, the outcome of your refusal, and the reason why you refused to submit to such a test.

No.

70. In the past ten years, have you suffered memory loss or impaired judgment for any reason? If so, please explain in full.

No.

SUPPLEMENTAL INFORMATION

71. Describe any additional education or experiences you have which could assist you in holding judicial office.

In addition to my legal experience and work in education, after assisting with the creation and implementation of Teen Court as noted in Q41, I also served for years as a judge and a mentor for cases diverted for hearings. It was a pleasure to work with student prosecutors and defense attorneys. I found the process of peer review to be quite interesting and effective. I would carefully consider the sentences handed down by the jury and impose appropriate sanctions based upon the case before me.

Additionally, I have assisted with several judicial elections which would assist me in holding and defending judicial office. I am familiar with the rules and regulations applicable to judicial campaigns. I have seen how important it is to a judicial campaign to follow the rules and to connect with the public.

I have served on several community boards and participated in multiple community organizations. Each experience has either allowed me to meet and learn from some amazing people, or it has allowed me to better myself and how I interact with the network of people needed to make organizations run effectively. In each of these positions, I have learned about leadership, integrity, decision-making, hard work, compassion, public trust, and commitment. Community service has been extremely rewarding for me and demonstrates my commitment to this community, a commitment I look forward to continuing as a circuit judge.

72. Explain the particular contribution you believe your selection would bring to this position and provide any additional information you feel would be helpful to the Commission and Governor in evaluating your application.

I often tell people that I am fortunate to have always been able to say that I "get" to go to work, rather than I "have" to go to work. I have spent my entire life, both in my work and personal life, seeking to help others. Public service is what initially drew me toward the practice of law and made me excited to get out of bed and go to work.

At the Attorney General's Office, I often received phone calls seeking guidance on substantive and procedural issues. Usually, the questions had tight, if not immediate, deadlines. I also developed strong research and analytical skills. Attention to detail, discerning the correct legal actions, and caseload management were always important. At ERAU, I help students learn about the law, life, and decision-making. Being a professor has improved my ability to listen, observe, analyze, and take appropriate actions. These capabilities will serve me well if selected to as a judge. A judge must be able to manage various aspects of the job simultaneously; my experience has prepared me to be successful in this regard. My respect for the position of circuit judge and its importance to governance and our community will foster a positive courtroom and culture. Judges must interpret the law as written, not as they would like it to be. As an appellate attorney, I understand well the need to rely only upon what the written word provides. Protecting the unique position of public trust judges occupy, I would work with all those involved in the judicial proceeding with respect and humility. I believe serving on the bench is the highest calling in the legal profession, but more importantly, it epitomizes service to the public.

I have managed caseloads and supervised people; I understand the law and legal system, have learned new skills and become proficient at them, and made difficult decisions. I believe my experience, both legal and non-legal, demonstrates that I possess the skills, knowledge, abilities, and temperament to be successful as a circuit judge.

REFERENCES

73. List the names, addresses, e-mail addresses and telephone numbers of ten persons who are in a position to comment on your qualifications for a judicial position and of whom inquiry may be made by the Commission and the Governor.

- The Honorable Leah R. Case, Chief Judge, Seventh Judicial Circuit, S. James Foxman Justice Center, 251 N. Ridgewood Avenue, Daytona Beach, Florida 32114, lcase@circuit7.org, (386) 239-7792

- The Honorable Christoper A. France, Seventh Judicial Circuit, Circuit Judge, Kim C. Hammond Justice Center, 1769 E. Moody Blvd., Bunnell, Florida 32110, cfrance@circuit7.org, (386) 313-4515

- The Honorable Wesley H. Heidt, Seventh Judicial Circuit, County Court Judge, Volusia County Courthouse Annex, 125 E. Orange Avenue, Suite 305, Daytona Beach, Florida 32114, wheidt@circuit7.org, (386) 257-6058

- The Honorable Raul A. Zambrano, Seventh Judicial Circuit, Circuit Judge (retired) P.O. Box 290034, Port Orange, Florida, 32129, [redacted]

- Chase Tramont, State Representative, Capitol Office, 1301 The Capitol, 402 S. Monroe St., Tallahassee, Florida 32399-1300, chase@chasetramont.com, (850) 717-5030 (work), [redacted]

- Lori Tolland, City Commissioner, Zone One, City Hall, 22 South Beach Street, Ormond Beach, Florida 32174, Lori.Tolland@gmail.com, [redacted]

- Patrick W. Krechowski, Esq., Balch & Bingham, LLC, One Independent Drive, Suite 1800, Jacksonville, Florida 32202, pkrechowski@balch.com, (904) 393-9000 (work), [redacted]

- Abraham C. McKinnon, Esq., McKinnon & McKinnon, P.A., 595 W. Granada Boulevard, Suite A, Ormond Beach, Florida 32174, amckinnon@mckinnonandmckinnonpa.com, (386) 677-3431

- Steve Ridder, Embry-Riddle Aeronautical University Head Men's Basketball Coach, 1 Aerospace Boulevard, ICI Center, Daytona Beach, Florida 32114, ridders@erau.edu, (386) 323-5025 (work)

- R. Andrew Watts, Executive Vice President, Chief Financial Officer & Treasurer, Brown & Brown, Esq., 300 North Beach Street, Daytona Beach, Florida 32114, awatts@bbins.com, (386) 239-8811

Q 22

Writing Samples

IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA

FIFTH DISTRICT

ROBERT LENTINO,
Appellant,

v. Case No. 5D21-2155

TORIANNE McKINNEY,
Appellee.
_____/

ON APPEAL FROM THE CIRCUIT COURT
OF THE SEVENTH JUDICIAL CIRCUIT
IN AND FOR VOLUSIA COUNTY, FLORIDA

INITIAL BRIEF OF APPELLANT

THE LAW OFFICE OF AARON
DELGADO & ASSOCIATES, PLLC

Aaron D. Delgado
Fla. Bar #796271
adelgado@communitylawfirm.com

Ann M. Phillips
Fla. Bar #978698
amphil1227@gmail.com
227 Seabreeze Blvd.
Daytona Beach, Florida 32118

COUNSEL FOR APPELLANT

TABLE OF CONTENTS

TABLE OF CITATIONS

CASES:

STATUTES:

STATEMENT OF THE CASE AND FACTS

Appellant, Robert Lentino (hereinafter either Appellant or Lentino), is appealing from the trial court's entry of a final order granting injunctive relief for protection against dating violence. (R 90-94).

Torianne McKinney (McKinney or Appellee) filed a Petition for Injunction for Protection Against Dating Violence on July 15, 2021. (R 6-12). In the petition McKinney posited she had known Appellant since May 2020. (R 7). She and Appellant were in a continuous relationship from July 2020 until July 2021; she characterized the relationship as one wherein there the expectation of affection or sexual involvement between the parties existed. (R 7). Her petition alleges four incidents of violence occurring May 20 (punched in right eye), June 6 (punched in right eye), July 1 (gun to head), and July 3 (cut with knife). (R 8-9). McKinney alleged she feared imminent violence because Appellant made several threats via text that he is going to find her and kill her. (R 10).

On July 15, 2021, the trial court issued a temporary injunction for protection against dating violence. (R 14).

An evidentiary hearing on the petition was held on August 17, 2021. (R 129-293). At the hearing, McKinney testified that she has known Appellant since May 2020. (R 134). She and Appellant were in a continuous relationship from July 2020 until July 2021; she characterized the relationship as one wherein there the expectation of affection or sexual involvement between the parties existed. (R 134-135).

In May 2021, McKinney and Appellant were arguing about texts between Appellant and another woman. McKinney provided that when she ran into her bedroom and Appellant came in and hit her in the face. A photograph taken by McKinney of the alleged injury was admitted. (R 95, 136-137). Appellee testified she did not report the incident to the police since Appellant is a police officer. (R 138).

At an unknown date, McKinney testified, Appellant sent her a text stating he could not wait to beat the f*ck out of her the next time he saw her and that he literally wanted to blow her brains out. (R 96, 157). Appellant later testified that he has no recollection of that text and could not locate the message. (R 268-269).

McKinney also testified that on July 1, 2021, Appellant came over to her house on his lunch break. Appellee heard Appellant and her mother speaking with one another. McKinney came over and opened the door. (R 140-141). Her mother asked Appellee if she wanted Appellant there. (R 141). Appellee testified she wanted him there and invited him in. (R 141, 169). McKinney yelled at her mother that she did not care what she thought and told her to leave. (R 141, 167). Once inside the apartment, she and Appellant began fighting. (R 141). Appellant stated that McKinney's mother had been rude, and that McKinney owed him oral sex. When McKinney refused, Appellant put his service weapon to her head. (R 141-142). She yelled at Appellant and said to never come back. (R 169). The next day, McKinney asked Appellant if he would go to lunch with her. (R 169).

McKinney testified that Appellant pulled her vehicle over using his patrol vehicle one night for no reason. (R 143-144). Appellant objected to the testimony as a violation of due process; the allegation was not part of the petition and had no notice. (R 143-144). The objection was overruled. (R 144).

McKinney testified that on July 3, she invited Appellant over and they were hanging out. (R 146, 169, 172). When Appellant began touching her in a sexual manner, she started "freaking out" and asked him to get her some water. Appellant got up and went into the kitchen. (R 146, 170-171). After he had been gone around five minutes, McKinney got up to get her own water. (R 146-147, 171). McKinney saw Appellant on his phone and asked what he was doing. (R 147). Appellant answered, "I'm on my f*cking phone." (R 147). She then grabbed her own water and turned to walk away saying something like "god, that's more important than me," when Appellant grabbed her arm while holding a knife in his hand. (R 147). When Appellant's pulled her toward himself, the knife cut her upper thigh. (R 147). She took a photograph of her injury which was viewed by the court. (R 147-153). Appellee left McKinney's residence around 6:30 that evening. (R 153). McKinney testified she sent Appellant a message around 3:00 AM telling him she was blocking him, and she did not want to hear from him again. (R 116, 153, 172). The text did not say anything about Appellant cutting McKinney or being violent. (R 116, 173). McKinney stated in the text that she was done with toxic games. (R 116, 173). It was the

official end of their relationship. (R 153-154). Since that time, Appellant has not tried to contact her other than a call from him and two other people to her to offer money to "delete everything and say that it was a lie." (R 154, 219-220, 222, 258-260). The "stuff" Appellant was referring to involved conversations Appellee was posting on social media between himself, Appellee and a girl named Hannah that referenced sex. (R 241-242). McKinney indicated she did not care that Appellant was upset and worried about his job by the postings and that he should be careful who he messes with if he did not want McKinney to "get you back ten times harder." (R 243).

McKinney reported the incident to police three days later, on July 7. (R 173-174). McKinney testified she did not remember law enforcement telling her that her story did not make sense, nor did she remember them confronting her about multiple cuts on her body. (R 174).

Daytona Beach Police Officer Mariah Acosta testified that she was called out on July 7 to a scene involving McKinney (R 187-188). Her role was taking photographs, among them were photos of McKinney's body. (R 188). McKinney had was appeared to be several healed lacerations on her stomach, some on her arm area,

her forearm area, another to her leg and a burn mark on her other leg as well as some bruising on knee, the back of her knee and her hand. (R 188). All the lacerations were healed. (R 188-189). The laceration on her thigh near the bikini area and the burn mark appeared to be the freshest. (R 188-189).

Christian Smith testified that he was friends with both Appellant and Appellee at one point. (R 200-201). He testified that on May 18, McKinney FaceTimed him stating she had taken all her pills, and could he help her. (R 203). He called emergency personnel seeking a wellness check on McKinney and headed to her residence. (R 203). At some point possible shortly before May 20, Mr. Smith had sent McKinney a text stating that Smith had seen Appellant making out with another girl. (R 204). Appellee did not take the news well. (R 205).

On June 30, the day before the alleged incident on July 1, Appellee called Mr. Smith telling him she had again taken some pills and needed help. (R 206-207). Smith reached out to Appellant, but Appellant could not go check on her, so Smith went to see McKinney. (R 207, 244). She was asleep when he arrived, but not in need of emergency assistance; she did not remember calling

Christian. (R 207). Mr. Smith texted about McKinney during the next several days because Smith was concerned for her safety. (R 208, 215). To the best of Smith's knowledge, Appellant and Appellee were not in a dating relationship; Smith testified McKinney was involved with other people. (R 210-211). McKinney told Smith that Appellant was violent with her. (R 211, 217). Smith did not believe it at first, but then started to see pictures and messages on social media. (R 211). Smith was aware that McKinney had been involved in abusive relationships in the past. (R 211-212).

Appellant, Robert Lentino, testified that he and McKinney were friends with benefits, meaning they were friends who would have sexual relations occasionally. (R 223-224). They often used words such as "bitch" and "ho" in joking terms to refer to each other. (R 225). Appellant testified he did not physically see McKinney on May 20 or June 6 because he was at work; his timesheets were admitted. (R 108-109, 226-231, 252).

Appellant explained texts between himself and Appellee from June 25 to July 4; they seemed complete and accurate. (R 233-235). On July 3, McKinney reached out to Appellant saying she needed help. (R 236). Appellant said he would come over; when he

did, she answered the door in her robe and undergarments. (R 237). She stated she did not feel well. (R 237). He kept asking her what was wrong, and she kept saying nothing. (R 237). He did not show up with an expectation of a sexual encounter. (R 237).

He tried to get her to go to Halifax. At one point, she agreed and wanted Appellant to drive her there. (R 239-240). Appellee changed her mind because the doctor wouldn't see her due to the time of day. (R 240). Lentino never went into the kitchen that visit, nor did he grab a knife. (R 240). He eventually saw a washcloth on McKinney's hip area but did not see what was under it. (R 240-241). He did not take a knife to her. (R 241). Neither did Appellant pull his service firearm, state he expected oral sex, or push McKinney against a wall. (R 248).

The next day, McKinney sent Appellant a text stating she was done with toxic relationships. Appellant believes this is based on the fact that he would not give her a "relationship title" like girlfriend. (R 242).

Appellant testified that he did pull Appellee's car over one time near his house. He saw a car that looked like hers, but also looked

suspicious; it was near his home and Appellee had never been to Appellant's home. (R 255-258).

After closings, the trial judge stated that the testimony was complicated and convoluted. He found the grounds for the injunction had "been met, without making other specified findings of facts as to which acts of violence or the severity of them or the purpose behind them." (R 292). The judge stated the traffic stop was disturbing, coupled with the testimony about offering to pay money to have materials taken off social media. (R 292-293).

Following the hearing, the trial court issued a final judgment of injunction for protection against dating violence. (R 90-94). In the form order, it is noted that the court finds that McKinney "is a victim of dating violence and/or [McKinney] has reasonable cause to believe he or she is in immediate danger of becoming a victim of an act of dating violence ... and that an immediate and present danger of dating violence exists to [McKinney]... ". (R 90). The injunction for protection was ordered to be in full force and effect until August 17, 2023. (R 91). As part of the injunction, the trial court ordered that Appellant not use or possess a firearm or ammunition. (R 92).

Appellant filed a notice of appeal on August 25, 2021. (R 122). An amended notice of appeal was filed August 26, 2021. (R 126).

SUMMARY OF THE ARGUMENT

The trial court abused its discretion in entering a final order for protection against dating violence against Appellant. Appellee failed to present competent, substantial evidence to support her request for a final injunction. Specifically, she failed to demonstrate that she had reasonable cause to believe she was in imminent danger of another, future act of dating violence. The court improperly considered allegations not set forth in Appellee's petition. Additionally, the facts do not support the trial court's imposition of the condition that Appellant not use or possess a firearm or ammunition during the term of the injunction.

The final injunction should be vacated, and the matter remanded for dismissal. Alternatively, the matter should be remanded for the removal of the requirement that Appellant not use or possess a firearm or ammunition during the term of the injunction.

ARGUMENT

THE EVIDENCE WAS LEGALLY INSUFFICIENT TO SUPPORT THE TRIAL COURT'S ENTRY OF A FINAL ORDER FOR PROTECTION AGAINST APPELLANT.

Appellant Robert Lentino (hereinafter either Appellant or Lentino) appeals the trial court's final judgment of injunction against dating violence entered against him in favor of Appellee, Torianne McKinney. Appellant contends the evidence presented at the final hearing was legally insufficient to support a finding that Ms. McKinney had a reasonable fear that she was in imminent danger of another act of dating violence.

While a final judgment of injunction is reviewed for a clear abuse of discretion, whether the evidence is legally sufficient to support the issuance of the injunction is reviewed *de novo*. Whitfield v. Meeks, 324 So. 3d 565, 568 (Fla. 1st DCA 2021) (citing Sumners v. Thompson, 271 So. 3d 1232, 1233 (Fla. 1st DCA 2019). Section 784.046(2)(b), Florida Statutes (2021), authorizes the issuance of an injunction against dating violence for the protection of "[a]ny person who is the victim of dating violence and has reasonable cause to believe he or she is in imminent danger of

becoming the victim of another act of dating violence." To obtain an injunction against dating violence, the petitioner must prove with competent, substantial evidence that she has reasonable cause to believe that she is in imminent danger of another, future act of dating violence. Nuila v. Stolp, 188 So. 3d 105, 106 (Fla. 5th DCA 2016); see also Schultz v. Moore, 282 So. 3d 152, 153 (Fla. 5th DCA 2019). "In determining whether reasonable cause exists, 'the trial court must consider the current allegations, the parties' behavior within the relationship, and the history of the relationship as a whole.'" Brungart v. Pullen, 296 So. 3d 973, 976 (Fla. 2d DCA 2020) (quoting Gill v. Gill, 50 So. 3d 772, 774 (Fla. 2d DCA 2010)).

The relevant portion of the dating-violence statute has two elements:

> Any person who is the victim of dating violence and has reasonable cause to believe he or she is in imminent danger of becoming the victim of another act of dating violence ... has standing in the circuit court to file a sworn petition for an injunction for protection against dating violence.

§ 784.046(2)(b), Fla. Stat. (2021).

The trial judge specifically referenced a traffic stop as an incident of concern. This incident, however, was not included in

McKinney's sworn petition for injunction against dating violence. (R 6-12). Florida Statute 784.046(4)(a) provides that the petition must allege the incidents of dating violence and must include "the specific facts and circumstances that form the basis upon which relief is sought." The trial court erred in ruling on matters not pleaded in the petition and testified to over Appellant's objection. In relying on matters outside the four-corners of the petition, the lower court violated Lentino's due process rights. Cook v. McMillan, 300 So. 3d 189, 193 (Fla. 4th DCA 2020) (citations omitted).

Similarly, the only "contact" between Lentino and McKinney since Appellee "ended" her relationship with Lentino on or around July 3, was a phone call wherein Lentino, with three other people on the call including Appellee, allegedly offered money to have Appellee get rid of photos and texts she had involving Appellant. This "contact" did not convey any threat of violence and occurred after the filing of the original petition. (R 154). Thus, this was not an incident which Appellee alleged created a well-founded fear of future violence.

The court only specifically noted the phone call and the traffic stop when entering the final order. As stated above, since the traffic

stop was not alleged in the petition for relief, it may not be relied upon by the trial court in its decision to grant or deny relief. Regardless, neither of these actions was violent. Neither establish by competent, substantial evidence that McKinney has a reasonable fear of imminent future violence. Cook, 300 So. 3d at 192. See Di Stefano v. Long, 279 So. 3d 758, 759 (Fla. 2d DCA 2019) ("[R]egardless of whether the petitioner has been the victim of dating violence in the past, the petitioner must show that he or she has reasonable cause to believe that he or she is in imminent danger of becoming the victim of an act of dating violence in the future." (citation omitted)).

Moreover, removing the traffic stop from the equation, the trial court only specifically relied upon one incident, the phone call, that was neither violent nor part of the petition. Based on the statute, "[i]t is not sufficient to have been the victim of one incident of dating violence in the past." Alderman v. Thomas, 141 So. 3d 668, 669 (Fla. 2d DCA 2014) (footnote omitted); see also Schultz v. Moore, 282 So. 3d at 153 ("[D]ating violence injunctions must be predicated on the reasonable prospect of a future violent act.").

Regarding the other facts, as the trial court noted, they were complicated and convoluted. The evidence demonstrated that McKinney was not in fear of Appellant but was angry that he would not commit to a relationship with her. The alleged injuries, a black eye and knife cuts, did not align properly with the testimony. The photo which was admitted into evidence did not show much injury to Appellee's eye and the injury that was shown was not consistent with the testimony of being punched in the eye. Appellee's prior history of cutting herself also undermined her allegations of knife injuries.

The facts of this case do not suggest that Appellant would continue to send messages or contact McKinney in the future. Appellant testified he has no intention or desire to speak to or see McKinney again. The evidence was not legally sufficient to demonstrate that McKinney had an objectively reasonable fear of imminent danger of a future act of dating violence.

Alternatively, neither of the two incidents specifically relied upon by the trial court involve a firearm. The court made no additional findings that this prohibition was necessary to secure McKinney's safety. An injunction should never be broader than is

necessary to secure the injured party. Chevaldina v. R.K./FL Mgmt., Inc., 133 So. 3d 1086, 1091 (Fla. 3d DCA 2014). This provision is not statutorily mandated and should only be included where required to protect the petitioner. Langner v. Cox, 826 So. 2d 475 (Fla. 1st DCA 2002). Since the trial court did not provide a reasonable basis for its requirement that Lentino not use or possess a firearm or ammunition, this requirement should be stricken from the final order should this court affirm the entry of the final order.

Based on the specific facts of this case, Lentino submits that the evidence was legally insufficient for a finding that McKinney had an objectively reasonable fear of imminent danger of becoming the victim of a future act of dating violence. Since the traffic stop was not included in the petition for injunctive relief, it may not be considered by the court in making its ruling. Likewise, the phone call should not be considered as supporting imminent future violence. The trial court's final order for injunction for protection against dating violence should be vacated and the case remanded for the entry of an order of dismissal.

Alternatively, should the court find that the evidence was legally sufficient to support the entry of the final order, the cause

should be remanded to the trial court for the provision regarding Lentino not being permitted to possess or use firearms or ammunition to be stricken.

CONCLUSION

Based upon the foregoing, Appellant respectfully requests this Honorable Court reverse the lower court's August 17, 2021, injunction for protection against dating violence and remand the case to the circuit court for the entry of a final judgment of dismissal.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing Initial Brief has been furnished by electronic service via the Florida Courts E-Filing Portal, and to Daniel M. Leising, Counsel for Appellee, at leisingd@gmail.com on this 10th day of January, 2022.

THE LAW OFFICE OF AARON DELGADO & ASSOCIATES, PLLC

/s/ Aaron D. Delgado
AARON D. DELGADO, ESQUIRE
Fla. Bar. #796271
adelgado@communitylawfirm.com

/s/ Ann M. Phillips
ANN M. PHILLIPS, ESQUIRE
Fla. Bar #978698
amphil1227@gmail.com

Delgado & Associates
227 Seabreeze Boulevard
Daytona Beach, Florida 32118
Telephone: (386) 255-1400
Facsimile: (386) 255-8100

COUNSEL FOR APPELLANT

CERTIFICATE OF COMPLIANCE FOR COMPUTER GENERATED BRIEF Fla. R. App. P. 9.045

I hereby certify that this brief was prepared using Bookman Old Style 14-point font and that it complies with the word count requirements in the Florida Rules of Appellate Procedure in that this initial brief contains less than 13,000 words.

/s/ Ann M. Phillips
Ann M. Phillips
Counsel for Appellant

IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA

FIFTH DISTRICT

MELODY L. DANIELS

Appellant,

v. CASE NO. 5D14-0599

STATE OF FLORIDA

Appellee.
_____/

ON APPEAL FROM THE CIRCUIT COURT
OF THE SEVENTH JUDICIAL CIRCUIT
IN AND FOR VOLUSIA COUNTY, FLORIDA

ANSWER BRIEF OF APPELLEE

PAMELA JO BONDI
ATTORNEY GENERAL

ANN M. PHILLIPS
ASSISTANT ATTORNEY GENERAL
Fla. Bar #978698
444 Seabreeze Blvd.
5th Floor
Daytona Beach, Florida 32118
(386)238-4990
(384)238-4997 (fax)
crimappdab@myfloridalegal.com

COUNSEL FOR APPELLEE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

STATEMENT OF CASE AND FACTS

Appellant's statement of the case and facts is substantially accurate for the purpose of this appeal. Appellee offers the following additions and/or corrections in support of this answer brief.

Deputy Jason Paul testified that he was working for the Volusia County Sheriff's Office, but had previously worked for the Florida Highway Patrol (FHP); he had a total of approximately 12 years of experience in law enforcement. (R 1360-1361, V7). Paul was working for FHP on the date of the crash in question. (R 1363, V7). The crash occurred on Interstate 95 at around 8:50 PM on January 2, 2012. (R 1363-1364, V7). The road is two lanes in both directions; the northbound side, where the accident occurred, is flanked on the right by an emergency shoulder and on the left with "wake-up" striping. (R 1365, V7). The northbound and southbound lanes are separated by a large, grassy median. (R 1365, V7). Photos of the area were published to the jury. (R 1369-1370 V7).

Upon arriving, Paul saw two vehicles in the median; both appeared to have rolled over, one was upside-down and one was on all four tires. (R 1370, V7). There were two people inside the victim-vehicle - the driver and a passenger. The driver was taken away by helicopter and Paul spoke briefly on-scene to the passenger. (R 1371, V7).

Paul spoke with Appellant while she was in the back of the

ambulance. (R 1371, V7). As they were speaking, Paul noticed a strong odor of alcohol upon Appellant's breath. (R 1371, V7). Appellant was very argumentative, insulting, and uncooperative. (R 1371, V7). Appellant's eyes were bloodshot and glassy. (R 1372, V7). Appellant's actions and appearance were consistent with one who is impaired: odor of alcoholic beverages on her breath; her bloodshot, watery, glassy eyes; her slurred speech; her belligerent attitude; and the vehicular crash. (R 1372, V7).

As a trooper, Paul investigated crashes on a routine basis - it constitutes about ninety percent of a trooper's job. (T 1373, V7). In addition to his 11 years of on-the-job experience, Paul had taken courses including advanced traffic homicide investigation courses. (R 1373, V7). Over ten years, Paul worked at least 5,000 crashes as a conservative estimate. (R 1374, V7). As part of his investigation, Paul did a reconstruction. (R 1374, V7). In preparing his reconstruction, Paul utilized evidence on the roadway: marks on the roadway, crush damage to the vehicle(s), debris, the final resting place of the vehicle(s), and statements of those involved. (R 1374, V7).

Paul explained skid marks and yaw marks, pointing out some in photos of the scene. (R 1376, V7). In examining the scene, Paul used his standard-issue police Maglite which is a powerful light. (R 1377, V7). Here, Paul walked the scene of the crash and beyond to ensure he covered the entire area. (R 1378, V7). Paul made a

diagram of the crash scene; the diagram, depicting Appellant's vehicle as Car 1, was shown to the jury. (R 1379-81, V7).

Paul explained that he knew Appellant's vehicle had caused certain yaw marks because the marks "make pretty much an arrow, like a big old neon sigh pointing to where [Appellant] landed." (R 1381, V7). The yaw marks began between the two lanes indicating the presence of Appellant's vehicle as the vehicle had to be there in order to make the marks. (R 1381-82, V7). Appellant's vehicle basically did a "pit maneuver" on the victim's vehicle. (R 1382-83, V7).

Paul saw evidence where both vehicles hit the grass. (R 1383, V7). A car could not drive on the area near the median as it was not wide enough. (R 1384, V7). Paul did not find any car parts which did not belong to the two vehicles. (R 1386, V7). Photos of both vehicles and the damage thereto were shown to the jury. (R 1390-92, V7). Appellant's vehicle did not have rear-end crush damage to the bumper, which is inconsistent with a vehicle which was rear-ended. (R 1393, V7). Appellant's vehicle contained no indications of where there was contact by a third vehicle; there was no paint transfer on the rear of Appellant's vehicle. (R 1393-94, V7). Paul knew of no vehicle which could cause the damage at the scene and not get wrapped up in the accident themselves. (R 1395, V7).

SUMMARY OF THE ARGUMENT

Appellant's argument was not preserved for appellate review. The State presented sufficient evidence a crime occurred. Reversible error has not been demonstrated.

ARGUMENT

THE TRIAL COURT DID NOT ERR IN DENYING APPELLANT'S MOTION FOR JUDGMENT OF ACQUITTAL AS THE STATE PRESENTED SUFFICIENT EVIDENCE REBUTTING THE DEFENSE'S HYPOTHESIS OF INNOCENCE.

Appellant, Melody Daniels (hereinafter either Appellant or Daniels), contends that the lower court erred when it denied her motion for judgment of acquittal as to the offense of driving under the influence causing serious bodily injury. Specifically, she argues the State failed to present evidence which refuted her reasonable hypothesis of innocence. As the State presented competent evidence which was inconsistent with Appellant's theory of events, Appellee respectfully submits that the trial court's ruling was proper.

PRESERVATION

Prior to addressing the merits of Appellant's arguments, Appellee contends that the arguments addressing Daniels' motion for judgment of acquittal for the offense of DUI with serious bodily injury has not been preserved for appellate review. In order to preserve the issue regarding a judgment of acquittal for appellate review, Florida Rule of Criminal Procedure 3.380(b) states that a motion for judgment of acquittal "*must fully* set forth the grounds on which it is based." (emphasis added.) Here, Daniels' motion for judgment of acquittal was inadequate because

it did not bring to the attention of the trial court any of the specific grounds he now urges this Court to consider. (T 516, V6). See Victorino v. State, 23 So. 3d 980 (Fla. 2009) (holding the claim of improper denial of a motion for judgment of acquittal had not been preserved for appeal by a boilerplate motion without specific grounds); Patterson v. State, 391 So. 2d 344 (Fla. 5th DCA 1980) (holding a bare-bones motion for directed verdict will not permit a defendant to raise every possible claimed insufficiency in the evidence). Rather, Daniels merely requested the court grant a motion for judgment of acquittal. (T 259, V8; T 371, V9). Without specific grounds, this matter is unpreserved for appellate review. See also Marquard v. State, 641 So. 2d 54 (Fla. 1994) (finding a particular argument not preserved as to the trial court's denial of motion for judgment of acquittal on a murder charge).

STANDARD OF REVIEW

On appeal, the appellate court reviews a motion for judgment of acquittal under a *de novo* standard of review. See Pagan v. State, 830 So. 2d 792, 803 (Fla. 2002); Tibbs v. State, 397 So. 2d 1120 (Fla. 1981). An appellate court will generally not reverse a conviction that is supported by substantial, competent evidence. See Donaldson v. State, 722 So. 2d 177 (Fla. 1998); Terry v. State, 668 So. 2d 954, 964 (Fla. 1996). If, after viewing the evidence in the light most favorable to the State, a rational trier of fact

could find the existence of the elements of a crime beyond a reasonable doubt, then there is sufficient evidence to sustain a conviction. See Banks v. State, 732 So. 2d 1065 (Fla. 1999).

When the State's case is wholly circumstantial, however, there must not only be sufficient evidence establishing each element of the offense, but the evidence must also be inconsistent with the defendant's reasonable hypothesis of innocence. See Pagan, supra; Orme v. State, 677 So. 2d 258 (Fla. 1996). The circumstantial evidence rule does not, however, require the jury to believe the defendant's version of facts when the State has produced conflicting evidence. Bedored v. State, 589 So. 2d 245, 250 (Fla. 1991). Further, the State is not required to rebut every possible variation of events which could be inferred from the evidence, but only to introduce competent evidence which is inconsistent with the defendant's theory of events. Kaczmar v. State, 104 So. 3d 990, 1002 (Fla. 2012). Once that threshold is met, it becomes a question for the jury. State v. Law, 559 So. 2d 187, 189 (Fla. 1989).

This Court, however, in Knight v. State, 107 So. 3d 449, 451 (Fla. 5th DCA 2013), questioned the applicability of the "special standard of review" in circumstantial evidence cases and questioned the need for a special standard of review. See also State v. Sims, 110 So. 3d 113, 117 (Fla. 1st DCA March 25, 2013)(Thomas, J. dissenting)(agreeing with "with the insightful

analysis expressed by Judge Lawson and the Fifth District in Knight [...] which recognized that the special standard of review in circumstantial-evidence criminal cases is inconsistent with the Florida jury instructions, federal law, and the majority of state jurisdictions."). Appellee submits that, based upon the existence of victims' statements and the physical damage to the vehicles and crash scene, the instant case is not a wholly circumstantial evidence case. If, however, this Court finds that the case is based on wholly circumstantial evidence, under Knight, the special standard of review should not apply. Nevertheless, even applying the special standard of review, Appellee submits that the issue of Daniels' guilt was properly submitted to the jury.

MERITS

Despite Daniels' failure to preserve this issue for appellate review, this Court may consider the issue under the fundamental error doctrine if "the evidence [was] insufficient to show that a crime was committed at all." F.B. v. State, 852 So. 2d 226, 230 (Fla. 2003). The evidence in the instant case was sufficient to convict Daniels of driving under the influence causing serious bodily injury. The elements of this offense are met if: (1) a person driving or in actual physical control of a vehicle, (2) who was under the influence of alcoholic beverages to the extent that the person's normal faculties are impaired or has a blood or breath alcohol level of .08 or more, (3) causes or contributes to causing

serious bodily injury to another person as a result of operating the vehicle. Bribiesca-Tafolla v. State, 93 So. 3d 364, 367 (Fla. 4th DCA 2012); Fla. Std. Jury Instr. (Crim.) 28.3 (2014); §§ 316.193(1), 316.193(3)(a), (3)(b), (3)(c) 2., Fla. Stat. (2013). Additionally, here, the jury found Daniels guilty of the lesser-included offense of driving under the influence causing injury. (R 1240, V7). As there was sufficient evidence of the greater charge, there was also sufficient evidence of this lesser charge.

Florida's supreme court has established clear rules that the courts must apply in evaluating the sufficiency of the evidence on a motion for judgment of acquittal. Unless "there is no view of the evidence which the jury might take favorable to the opposite party that can be sustained under the law," the trial court should not grant the motion. Williams v. State, 967 So. 2d 735, 755 (Fla. 2007) (quoting Gudinas v. State, 693 So. 2d 953, 962 (Fla. 1997)). The existence of contradictory, conflicting testimony or evidence "does not warrant a judgment of acquittal because the weight of the evidence and the witnesses' credibility are questions solely for the jury." Fitzpatrick v. State, 900 So. 2d 495, 508 (Fla. 2005). "Where there is room for a difference of opinion between reasonable men as to the proof of facts from which the ultimate fact is sought to be established," the force of such conflicting testimony should not be determined on a motion for judgment of acquittal. Darling v. State, 808 So. 2d 145, 155 (Fla. 2002). Once

the State presented evidence that was inconsistent with the defense's theory of events and from which a jury could infer guilt to the exclusion of all other inferences, it became a question for the jury to decide. See Orme v. State, 677 So. 2d 258, 262 (Fla. 1996).

While Daniels now contends on appeal that the judgment of acquittal should have been granted below based upon the State's failure to rebut her hypothesis of innocence, i.e., the third vehicle, the State's case did contain evidence which contradicted her theory. The testimony from Deputy Paul contradicts the defense's position that a third car was the cause of the crash. It was proper for the judge to allow the jury to decide the matter.

Viewing the evidence, and all reasonable inferences therefrom, in the light most favorable to the State, the prosecution presented competent evidence which rebutted Daniels' hypothesis of innocence of third-car causation. Since the credibility and probative force of conflicting testimony should not be determined on a motion for judgment of acquittal, the trial court properly submitted the issue of Daniels' guilt to the jury. Reversible error has not been demonstrated.

CONCLUSION

Based on the arguments and authorities presented herein, Appellee respectfully requests this Honorable Court affirm the judgment and sentence in all respects.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the above and foregoing Answer Brief of Appellee has been furnished to counsel for Appellant, Assistant Public Defender Christopher S. Quarles, 444 Seabreeze Boulevard, Suite 210, Daytona Beach, Florida 32118, by email at appellate.efile@pd7.org and quarles@pd7.org, this 12th day of November, 2014.

DESIGNATION OF EMAIL

I HEREBY DESIGNATE the following email addresses for purposes of service of all documents, pursuant to Rule 2.516, in this proceeding: crimappdab@myfloridalegal.com (primary) and ann.phillilps@myfloridalegal.com (secondary).

CERTIFICATE OF COMPLIANCE

I HEREBY CERTIFY that this brief was typed in 12-point Courier New as required by Rule 9.210(a)(2).

Respectfully submitted,

PAMELA JO BONDI
ATTORNEY GENERAL

/s Ann M. Phillips

ANN M. PHILLIPS
ASSISTANT ATTORNEY GENERAL
Fla. Bar #978698
444 Seabreeze Boulevard
5th Floor
Daytona Beach, FL 32118
(386) 238-4990/FAX (386) 238-4997
ann.phillips@myfloridalegal.com
crimappdab@myfloridalegal.com

Q 35

Published Articles

THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics,
Security and Law

Volume 15

Article 2

August 2020

Cryptography, Passwords, Privacy, and the Fifth Amendment

Gary C. Kessler
Gary Kessler Associates / Embry-Riddle Aeronautical University - Daytona Beach, kessleg1@erau.edu

Ann M. Phillips
Embry-Riddle Aeronautical University - Daytona Beach, ann.phillips@erau.edu

Recommended Citation
Kessler, Gary C. and Phillips, Ann M. (2020) "Cryptography, Passwords, Privacy, and the Fifth Amendment," *Journal of Digital Forensics, Security and Law*: Vol. 15 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2020.1678
Available at: https://commons.erau.edu/jdfsl/vol15/iss2/2

CRYPTOGRAPHY, PASSWORDS, PRIVACY,AND THE FIFTH AMENDMENT

Gary C. Kessler[1], Ann M. Phillips[2]
[1]Embry-Riddle Aeronautical University
Gary Kessler Associates
Ormond Beach, FL
[2]Embry-Riddle Aeronautical University
Daytona Beach, FL
gck@garykessler.net, ann.phillips@erau.edu

ABSTRACT

Military-grade cryptography has been widely available at no cost for personal and commercial use since the early 1990s. Since the introduction of Pretty Good Privacy (PGP), more and more people encrypt files and devices, and we are now at the point where our smartphones are encrypted by default. While this ostensibly provides users with a high degree of privacy, compelling a user to provide a password has been interpreted by some courts as a violation of our Fifth Amendment protections, becoming an often insurmountable hurdle to law enforcement lawfully executing a search warrant. This paper will explore some of the issues around this complex legal and social issue, including the evolution in the use of digital cryptography and the evolving legal interpretations of privacy.

Keywords: Cryptography, Fifth Amendment, Law, Passwords, Privacy, Self-incriminating testimony

1. INTRODUCTION

While addressing cybersecurity conference attendees at Boston College in 2017, then-FBI Director James Comey observed that the ubiquitous availability and use of strong cryptography was upsetting the delicate balance between privacy and security that is at the very heart of the U.S. social contract (Armerding, 2017). In 2019, Manhattan District Attorney Cyrus Vance, Jr. testified that strong iPhone encryption was Apple's "gift to sex traffickers" ("Written Testimony", 2019, para. 13). Today's digital cryptography truly is military-grade and provides an often insurmountable barrier for law enforcement when trying to execute a search warrant. This raises several questions:

1. How do we, as a society, feel about citizens having access to strong encryption and devices that are impervious to a government-sanctioned search?
2. Did the authors of the Constitution envision a container that could never be opened and, therefore, never be searched?
3. Is compelling a user to provide a password a violation of Fifth Amendment protections?

4. Should crypto products have backdoors for just these reasons?

This paper will explore these issues by examining the growing capabilities of cryptography (Section 2) and the evolving interpretation of privacy and self-incrimination (Section 3). Section 4 will discuss some of the issues as privacy and the needs of the state collide. Section 5 will provide some conclusions.

2. SOME MAJOR EVENTS IN DIGITAL CRYPTOGRAPHY

Cryptography is the science of writing in secret codes. Most historians point to the use of non-standard hieroglyphics in Egypt in 1900 B.C.E. as the beginning of secret code writing although that practice probably appears spontaneously soon after writing was developed (Kahn, 1996; Singh, 1999).

For several thousand years, the primary use of cryptography was for secrecy (aka privacy and confidentiality). It was also the exclusive domain of the literate and, even then, employed almost solely at the nation-state level to protect diplomatic communication and military secrets (Kahn, 1996; Singh, 1999).

While many advances in cryptographic codes appeared in the 1800s, one of the most notable practical contributions came from Auguste Kerckhoffs, a Dutch linguist and cryptographer. In 1883, Kerckhoffs proposed a number of design principles for military ciphers. One that maintains significance today says that the cryptographic system must not rely upon the secrecy of the encryption algorithm but upon the judicious choice, use, and storage of the keys. In fact, it is best to assume that the enemy knows the algorithm (Kahn, 1996; Kerckhoffs, 1883a, 1883b).

Cryptography continued to play a major role in diplomatic and military communication in the 20th century, playing a key role in the military campaigns of both World Wars (Haufler, 2003; Yardley, 1931). Commercial use of crypto, while introduced in the 1920s, started to grow so rapidly in the post-WW II era that the U.S. and most of the allied countries limited its use by civilians. In the U.S., in particular, cryptography was classified as a munition, which placed strict export controls on those products (Kahn, 1996; Levy, 2001).

The 1950s saw the dawn of the computer age in commercial organizations, notably in the financial industry. In the early 1970s, the National Bureau of Standards (NBS, now the National Institute of Standards and technology [NIST]) put out a call for a national standard encryption scheme for use with computers. The Data Encryption Standard (DES), designed by IBM and derived from an earlier IBM cipher called Lucifer, was adopted in 1977 and published as Federal Information Processing Standard (FIPS) Publication 46. The National Security Agency (NSA) had input into the development of DES, which caused many to wonder if they had implemented some sort of backdoor, a purposeful weakening of the algorithm to make is more susceptible to certain kinds of attack. Ironically, the NSA-designed Substitution (S)-boxes removed a mathematical weakness, making the algorithm stronger. However, IBM offered both 56- and 128-bit key versions of DES and the NSA insisted upon use of the smaller key, making it more susceptible to brute force attacks (Schneier, 2004).

Upon adoption, DES became the newest secret key cryptography (SKC) scheme. SKC, also called *symmetric cryptography*, uses a single key for both encryption and decryption. The key, then, is a shared secret between the sending and receiving parties. An important aspect of SKC schemes is the process of key exchange; specifically, how do the sender and

receiver share the key and keep it a secret? In 1977, the best way might be for one party to write it down and send it by armored car to the other party, using the same keys for days or weeks at a time (Kahn, 1996; Singh, 1999).

During this same era, Whitfield Diffie and Martin Hellman proposed a new form of encryption called public key cryptography (PKC). Also called *asymmetric cryptography*, PKC employs two keys, one to encrypt and the other to decrypt. Although the two keys are mathematically related and created as a pair, deriving the value of one of the keys by knowing the value of the other is computationally infeasible. Thus, one of the keys could be widely published and shared, known as the *public key*, while the other key remained a closely held *private key* (Diffie & Hellman, 1976).

The description of PKC was widely hailed as the biggest advance in encryption in hundreds of years. For 4,000 years, encryption was used almost solely to keep secrets. PKC could also provide sender authentication, message integrity, key exchange, and non-repudiation. In terms of key exchange alone, public key methods allowed secret keys to be generated and exchanged in milliseconds (Kahn, 1996; Levy, 2001).

PKC depends upon the existence of trapdoor functions. In this context, a *trapdoor* (as opposed to a *backdoor*) refers to a mathematical function that is easy to compute but where the inverse function is significantly harder to calculate; e.g., it is easier to perform exponentiation than it is to calculate logarithms and multiplication is easier than factorization. The first workable PKC algorithm was published by Rivest, Shamir, and Adleman (1978) and led to the first commercial PKC product, RSA.

In June 1991, Phil Zimmermann uploaded Pretty Good Privacy (PGP) to the Internet. PGP was the first open cryptosystem, combining hashing, compression, SKC, and PKC into a method to protect files, devices, and e-mail. Public keys were shared via a concept known as a Web of Trust; individuals would directly exchange their public keyrings and then share their keyrings with other trusted parties (Zimmermann, 2001).

PGP secret keys, however, were 128 bits or larger, making it a *strong* cryptography product. Export of strong crypto products without a license was a violation of International Traffic in Arms Regulations (ITAR) and, in fact, Zimmermann was the target of an FBI investigation from February 1993 to January 1996. Yet, in 1995, perhaps as a harbinger of the mixed feelings that this technology engendered, the Electronic Frontier Foundation (EFF) awarded Zimmermann the Pioneer Award and *Newsweek Magazine* named him one of the 50 most influential people on the Internet (Sussman, 1995; Zimmermann, n.d.).

With the commercialization of the Internet and dawning of the World Wide Web in the early 1990s, the government realized that there were legitimate needs for public use of strong cryptography. But not without government oversight. In 1993, at the same time as the Zimmermann investigation, NIST and the NSA introduced the Capstone project to provide strong crypto for public use. Capstone comprised several components (Crypto Museum, 2018; Kessler, 2020):

1. *Skipjack:* An SKC block cipher using an 80-bit key, the design of which was classified (a violation of Kerckhoffs' design principle described above)

2. *Clipper:* A tamper-proof computer chip that ran Skipjack, designed with a government-accessible backdoor

3. *Escrowed Encryption Standard (ESS):* A scheme whereby private keys would

be escrowed by NIST and the Treasury Dept.

Irrespective of the government's intentions, pushback against Capstone from privacy advocates and critics of its poor cryptographic practices – including the discovery of a flaw in the Clipper chip's law enforcement backdoor – resulted in the termination of the project by 1996 (Blaze, 1994; Meeks, 1994). Ultimately, Capstone was never adopted (EPIC, n.d.b).

By 1995, electronic-commerce (e-commerce) started to blossom on the Internet. At that time, many people – including the first author of this paper – were actually sending credit card numbers and other private information in unencrypted emails. All of this changed in 1995 with Netscape's release of the Secure Sockets Layer (SSL) protocol, an encryption enhancement employed by the Hypertext Transfer Protocol (HTTP) in Web servers and browsers that were fundamental to supporting the growth of commercial activity on the Internet. Because export of 128-bit keys was still prohibited, browsers in this era – including Internet Explorer and Netscape – had a domestic version with 128-bit keys and an international version with 40-bit keys. In 1996, however, President Bill Clinton issued Executive Order (EO) 13026, re-classifying crypto products as technology rather than munition, which greatly relaxed export controls and key sizes (Clinton, 1996; U.S. Dept. of Commerce, 2000).

While this sea change was ongoing in the mid-1990s, Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson, and Wiener (1996) released a white paper demonstrating that 56-bit keys were too short for practical, commercial purposes and that SKC schemes needed to use longer keys (Figure 1). Given that DES had had a 20-year lifetime in 1996, they concluded that the minimum key size for another twenty years was at least 75 bits.

Showing that 56-bit keys were insufficient was also a harbinger that the useful life of DES was coming to an end. In March 1998, NIST reaffirmed the DES standard for use for one additional five-year cycle but stated that a new standard would be developed. In July, however, the EFF introduced Deep Crack, a chip that could be built for $220K and brute force a DES key in an average of 4.5 days (EFF, 1998). This development effectively killed DES and caused a scramble as interim fixes and variants to DES became available (Kessler, 2020).

The process of developing NIST's next-generation SKC standard, called the Advanced Encryption Standard (AES), started in 1997. The AES process was handled very differently from the one that gave us DES. Whereas DES was developed under a shroud of secrecy, the AES process was an open, international competition. Fifteen proposals were submitted and reviewed, with all algorithms, documentation, and tests were posted on a NIST Web site. In 2001, an algorithm named Rijndael (developed by Belgian cryptographers Joan Daemen and Vincent Rijmen) – employing a 128-, 192-, or 256-bit key – was adopted as FIPS Pub. 197 (NIST, 2018).

It is worth noting several other crypto developments that occurred in the 2000s. Apple's Mac OS X, based on the Unix operating system, became available in 2001 (Painter, 2019). Mac OS X 10.3 (Panther) introduced FileVault in 2003, which could encrypt a user's home directory (Apple Inc., 2003). FileVault 2, a re-design of the original, was released in 2011 with Mac OS X 10.7 (Lion) and supported full startup volume encryption. This product was one of the first to employ AES encryption (Apple Inc., 2018; OSXDaily, n.d.).

In 2004, TrueCrypt, open source encryption for Windows, MacOS, and Linux, was released (TrueCrypt, 2015). TrueCrypt pro-

Attacker	Budget	Tool	Time Per Recovered Key 40-bit	56-bit	Key Length For Protection In Late-1995
Pedestrian hacker	Tiny	PC	1 week	Never	45
	$400	FPGA	5 hours	38 years	50
Small business	$10K	FPGA	12 min.	18 mon.	55
Corporate Dept.	$300K	FPGA	24 sec.	19 days	60
		ASIC	0.18 sec.	3 hours	
Big Company	$10M	FPGA	7 sec.	13 hours	70
		ASIC	5 ms	6 min.	
Government	$300M	ASIC	0.2 ms	12 sec.	75

ASIC = Application-specific integrated circuit
FPGA = Field programmable gate array

Figure 1. Effective key lengths for commercial applications (Adapted from Blaze et al., 1996)

vided a novel capability called *plausible deniability* (Figure 2). When a TrueCrypt encrypted volume is created, the user can define a single encrypted container or two encrypted containers using different passwords. Because the encrypted volume is randomized, it is not possible to tell whether there is a single container or two. If somehow compelled to provide a password, a user can supply the password to the standard TrueCrypt volume and there is no way to know if there is a hidden volume within (TrueCrypt Foundation, 2012). (On 28 May 2014, the TrueCrypt Web site suddenly went dark, announcing that the software was no longer being maintained and that users should seek alternatives. The story of TrueCrypt and the software that followed is beyond the scope of this paper but certainly an interesting twist.)

With the growth in the use of smartphones and the prodigious amount of personal information they contain, default encryption of these devices was inevitable. In 2014, Apple announced that iOS 8 devices would be encrypted by default and Google announced the same for Android 5.0 (Lollipop) (Miller, 2014).

3. SOME MAJOR EVENTS IN THE NOTIONS OF PRIVACY

Although the word "privacy" never appears in the U.S. Constitution or the Bill of Rights, Zimmermann – the author of PGP – suggests that privacy is an inalienable right that was understood by the framers (1999). Given the technology available in the late-1780s, any two people having a conversation knew whether they had privacy or not simply by looking around; if a third person came within earshot, the two people could merely walk away. The printed word was always visible. People had privacy because physics sup-

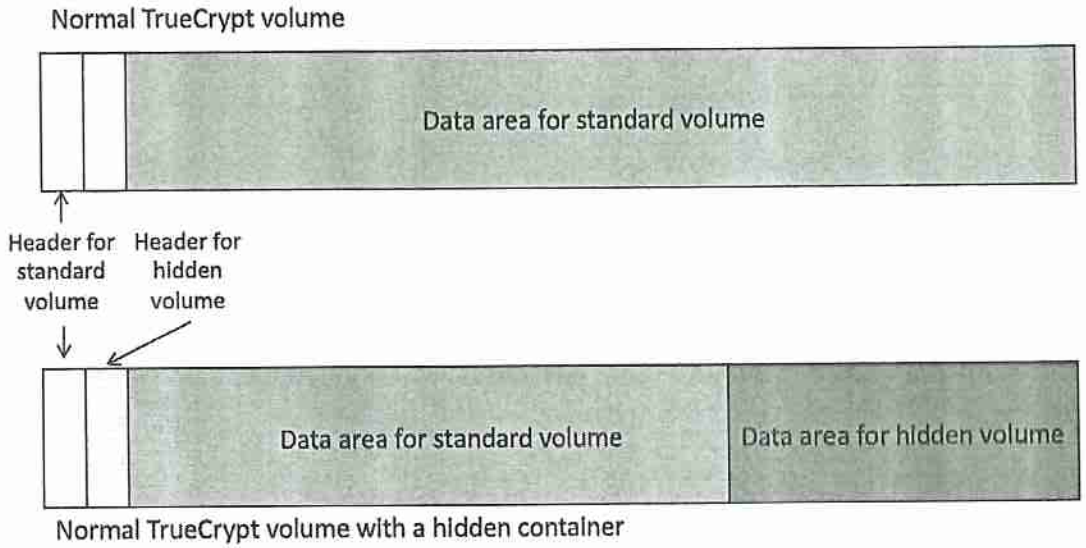

Figure 2. Plausible deniability in TrueCryp

ported it; the framers would no more discuss the right of privacy than they would the right to breathe air.

Most people today associate our expectation of privacy with the Fourth Amendment:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const. amend. IV).

One hundred years after the ratification of the U.S. Constitution, the invention of the camera – and an invasive press – brought the concept of privacy into public discussion. The right to privacy was first described by Warren and Brandeis (1890) and introduced the foundational concept that most Americans just want the "right to be let alone."

The Fourth Amendment protects against overly invasive government searches but also provides guidelines around when the government *can* access an individual's personal effects. In particular, a *search* is an:

1. Action by the state
2. Infringes upon one's reasonable expectation of privacy
3. Is legal only if there is a search warrant *or* a valid warrant exception

In this regard the Fourth Amendment can be viewed as involving a level of "taking" some level of privacy by a government entity.

The understanding of Fourth Amendment protections has changed over time with the current decisional law suggesting that they apply to people, not places (*Katz v. U.S.*, 1967; *Olmstead v. U.S.*, 1928). *Katz* also provides a guideline of what "reasonable expectation of privacy" means; namely, a *subjective expectation of privacy that is objectively reasonable.* This standard is met if

a person expects privacy (subjective) and society agrees that that expectation is reasonable (objective). As an example, a person standing inside of an enclosed, glass phone booth might have a reasonable expectation of privacy for a telephone conversation but probably does not have a reasonable expectation of privacy if they are taking their clothes off.

The Electronic Communications Privacy Act (ECPA, 1986), which governs electronic surveillance in the United States, has always drawn a distinction between user data and transactional data. *User data*, also called *content*, is the information that is under direct control of the user, such as the words typed into a file or words said during a telephone conversation. *Transactional data*, also called *non-content*, is the metadata needed by an entity such as a communications carrier, file system, or operating system to actually control or manage the data flow. The distinction between user content and metadata is consistent with the established legal doctrines regarding the privacy of content and the sharing of date under the third-party doctrine. By refusing to include content in the electronic surveillance data, the traditional *Katz* doctrine is being followed. Similarly, allowing metadata to be included in electronic surveillance comports with the third-party doctrine.

The third-party doctrine emanated from *Smith v. Maryland* (1979). In this case, Smith stole a woman's purse. A few days later, the woman started to receive harassing phone calls. Following the procedures of the ECPA, police placed a trap and trace device on her line to determine the numbers calling the woman; this process linked calls to Smith's number. Again, following ECPA provisions, police placed a pen register on Smith's line, showing that he was calling the woman. Smith was arrested, tried, and convicted. He appealed the conviction by asserting his expectation that his telephone calls were private. The Court upheld conviction, noting that a) police did not view the content of his calls and b) he had already shared the fact that he was calling the woman with a third party, namely the telephone company. These points are important to this discussion largely because metadata is typically not encrypted while content might be. Thus, metadata would seemingly always be available to law enforcement; it is content where the issue of encryption might be directly at issue. And content is where incriminating and exculpatory evidence of crime would be found.

The Fifth Amendment addresses, among other things, issues related to self-incriminating testimony and says, in part, "No person... shall be compelled in any criminal case to be a witness against himself" (U.S. Const. amend. V). This concept was novel at the time because the prevailing jurisprudence in the 1700s was that a suspect was guilty until proven innocent. The U.S. system of criminal justice is based upon the notion that a defendant is innocent until proven guilty and the state has the burden of proving guilt beyond a reasonable doubt. In this way, the Fifth Amendment can be seen as protecting against a person having to "give" evidence. Not forcing a defendant to testify is a way of implementing this precept; a criminal suspect does not have to speak and not speaking is not an implication of guilt.

Fisher v. U.S. (1976) introduced two relevant clarifications to Fifth Amendment protections, namely the Act of Production Doctrine and the Foregone Conclusion Doctrine. The Act of Production Doctrine says that a compelled act is testimonial when the act asserts information – i.e., the contents of one's mind – with some aspect of communication. In this case, the Court observed that *doing* something can convey information the same

as *saying* something. Thus, if a teacher asks a group of students to raise their hands if they read a certain paper, the act of raising the hand is testimonial since it conveys information that is in the students' heads. Courts have, therefore, come to interpret the Fifth Amendment as protecting both forms of compulsion, namely, testimony and production.

It is important to note that knowing a password and knowing the contents of an encrypted device are two different things. It is often the case people besides the owner of a device may know or be aware of the code needed to unlock the device; family members and friends, for example, often exchange or share this information for myriad reasons. Therefore, knowledge of a password is not a valid test that the person actually knows the contents and, therefore, is not in and of itself incriminating.

The Act of Production Doctrine considers a person's communication implicit in the act, not what communications may result from the act. How incriminating the production may be, or what the computer does when a person unlocks is, does not change the testimony implicit in the act of unlocking it. *In re Search Warrant Application* (2017) notes that use of biometry to access a device does not gain testimonial significance based on the information revealed; such an argument "...relies on conflating what it means for an act to be inherently testimonial versus an act yielding an incriminating result" (Section II, para. 11). In a sense, the passcode is akin to a fingerprint or a physical key; it can be used to open the device to further exploration, but neither the code nor the fingerprint nor the physical key creates any information to be decrypted; the information either exists or it doesn't irrespective of the unlocking of the device. Thinking of the issue in this regard overcomes the dichotomy of being able to use a fingerprint to unlock a device, but not obtain a passcode.

The Foregone Conclusion Doctrine says that compelling a person to produce information under certain circumstances is not testimonial if the state already, independently knows that the person has the information. So, as an example, if the state compels a person to open a safe by using a combination, the *act* of entering the correct combination is not incriminating testimony that the person knows the combination if the state can show that it had authentic, *a priori* knowledge that the person knew the combination. The elements of the Forgone Conclusion Doctrine are met when:

1. The state has knowledge of the existence in some specified location of the demanded evidence (*reasonable particularity)*
2. The person is known to have possessed or controlled the evidence
3. The evidence is authentic

The Foregone Conclusion Doctrine has two elements that apply more to the access to and acceptance of physical documents than to digital passwords. Reasonable particularity, the first such element, is a level of specificity that does not really apply to passwords; the state is seeking a single password with which to access a single device (*Commonwealth v. Jones*, 2019; Kerr, 2018; *U.S. v. Spencer*, 2018). The other element, authenticity, should not be an issue with passwords since they are self-authenticating; if the password works, it is clearly authentic (*Commonwealth v. Gelfgatt*, 2014; *In the Matter of the Search*, 2018; *State of Florida v. Stahl*, 2016).

Doe v. U.S. (1988) provides additional insight into when Fifth Amendment protections attach. According to *Doe*, "...an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information" (*Doe*, para. 3) in order to be

considered testimonial. Thus, Fifth Amendment privileges can only be invoked when these three elements apply:

1. Compulsion
2. Testimonial communication or act
3. Incrimination

Without these components, there is no Fifth Amendment issue. Per *Doe* (1988), "If a compelled statement is 'not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence'" (footnote 6). This relates to the question about whether providing a passcode is testimonial. If the initial compelled communication is testimonial, then any derivative evidence would be inadmissible; if, however, such information is not testimonial, then any derivative information would be properly admitted into evidence.

U.S. v. Hubbell (2000) further clarifies the limits of the Fifth Amendment. As part of a plea agreement, Hubbell agreed to provide certain documents relevant to a government investigation. After the government issued a subpoena to Hubbell to produce those documents, he asserted his Fifth Amendment privilege against self-incrimination before a Grand Jury. The prosecutor obtained a court order for the documents and offered immunity to Hubbell who, in turn, provided the documents, thus was in compliance with the original plea bargain. The government then used the documents to indict Hubbell for additional crimes. The Supreme Court dismissed the indictment, observing that the Fifth Amendment privilege against self-incrimination protects an individual from being compelled to disclose the existence of, much less produce, incriminating documents of which the prosecution has no *a priori* knowledge, thus is unable to describe with reasonable particularity. The Court also ruled that if an individual produces such documents pursuant to a grant of immunity, the government may not use them to pursue additional criminal charges against that person.

4. PRIVACY V. THE NEEDS OF THE STATE

The evolution and widespread availability of strong cryptography made it inevitable that an individual's expectation of privacy would be on a collision course with the legitimate needs of the state to execute a valid search warrant.

4.1 Compelling an Individual's Password

Since the early days of PGP, everyone from pundits and researchers to legal scholars and technocrats have wondered, "What happens if law enforcement issues a search warrant for an encrypted device and the user chooses not to comply?" It took more than 15 years for a court case to address this question (Nakashima, 2008).

U.S. v. Boucher (2007, 2009) is the first known case in the U.S. involving an encrypted computer and the question of self-incrimination. Boucher, a Canadian citizen, was stopped at a U.S. border crossing in Vermont. Upon examination, images of child pornography were found on his computer, which was encrypted using PGP Desktop software. The computer was powered down upon seizure and was unable to be further examined by law enforcement (Cohen & Park, 2018; Nakashima, 2008; Sacharoff, 2018). Police then asked a judge to compel Boucher to provide the password. In 2007, a U.S. Magistrate Judge ruled that compelling a password violated Boucher's Fifth Amendment protections against self-incrimination. Upon the government's appeal in 2009, a U.S. District Judge ordered Boucher to supply police with

an unencrypted version of the hard drive. At that point, Boucher accepted a plea agreement, was sentenced to three years in prison, and then subsequently deported.

During public discourse of the various Boucher rulings, many physical world analogies were made to this cyber world case. Most notably, the password was the same as a key to a locked room; providing the key is not incriminating even if the contents of the room are. But, in light of the Act of Production Doctrine, is revealing the key's location testimonial? One can be compelled to give a fingerprint, cheek swab, hair sample, blood, or other DNA; why not a password? But, perhaps a more fundamental question: Did the framers of the Constitution in 1878 ever conceive of a Fourth Amendment container that could not somehow be opened by physical means?

When applying for search warrants for physical documents, the government needs to meet the constitutional threshold of probable cause, i.e., that there is a fair probability that a search will result in evidence of a crime being discovered (U.S. Const. amend. IV). The government must also, as specific as is possible, describe the place to be searched, and the persons or things to be seized. The standard for searching for data on a digital device should not be higher. The standard for compelling the production of a password does not have to do with the eventual recovery of evidence. Rather, as some courts have held, the proper question is whether the government can demonstrate that it is a foregone conclusion that the defendant can decrypt the device (Kerr, 2018, 2019; *U.S. v. Apple MacPro Computer*, 2017).

The Foregone Conclusion Doctrine was significant in the Boucher Order. Boucher accessed his laptop at the Immigration and Customs Enforcement (ICE) agent's request at the border, where the agent ascertained the presence of child pornography. Because of that act, the Government knew of the existence and location of the hard drive and its files. Compelling Boucher to provide access to the unencrypted drive did not add to the sum total of the Government's information about the presence of possibly incriminating files (Kerr, 2019; Sacharoff, 2018; *U.S. v. Boucher*, 2009).

In addition, Boucher's act of producing an unencrypted version of the drive was not needed to authenticate it since he had already admitted to possession of the computer and provided the Government access to the drive. Since the Government could link Boucher with the files on his computer without making use of his production of an unencrypted version of the drive and stated that it would not use his act of production as evidence of authentication, there was no violation of his Fifth Amendment privileges (Kerr, 2018; *U.S. v. Boucher*, 2009).

The Boucher case did not provide guidance necessarily followed by other courts. In a similar case five years later in Massachusetts, suspect Gelfgatt was charged with multiple counts of forgery. Relevant evidence was known to be on his computers. Prior to trial, a motion to compel Gelfgatt to "...enter his password into encryption software" was denied by a Superior Court judge, who referred the point of law to the Supreme Judicial Court (SJC). The SJC reversed the denial, arguing that the motion violated neither the Fifth Amendment nor Article 12 of Massachusetts Declaration of Rights since the compelled decryption would not communicate facts of a testimonial nature beyond what Gelfgatt had already admitted to investigators (*Commonwealth v. Gelfgatt*, 2014).

Yet, five years after that, the state issued a *Gelfgatt* order for Jones – indicted for sex trafficking – to "provide... in writing... the PIN code" to a mobile phone (*Commonwealth v. Jones*, 2019). But *entering* and *revealing* a password are different things, and revealing

the password is not supported by *Gelfgatt*. Once the Commonwealth changed the request to entering the password, the order was upheld due to the Foregone Conclusion Doctrine (Kerr, 2019).

Requiring the disclosure of a password can be compared to the required disclosure of a private document, which may have some Fifth Amendment protection. The required oral disclosure of a password is often equated to incriminating testimony which is proscribed by the Fifth Amendment (Kerr, 2019).

Inconsistencies in rulings have appeared within states and between federal courts. Two cases in Florida provide a classic example. In *State of Florida v. Stahl* (2016), Stahl was arrested for video voyeurism (in this case, taking upskirt photos) in Sarasota. Stahl gave consent for the search of his mobile phone, confirmed the phone number, and provided police with the location of the phone – and then withdrew consent. The State's motion to compel Stahl to provide the password to police officers was denied by the trial judge, yet Florida's Second District appellate court quashed the trial judge's order, allowing the State to compel the password (Kerr, 2019).

In 2018, G.A.Q.L., a 17-year-old, was an inebriated driver in a high-speed collision in the southeastern part of the state, resulting in the death of a passenger in his vehicle (*G.A.Q.L. v. State of Florida*, 2018). The State made a motion to compel an iPhone 7 and iTunes password pursuant to a search warrant for the phone, for which they had credible belief that relevant evidence would be found. The trial court ordered the passwords to be provided, per *Stahl*. In this case, Florida's Fourth District appellate court quashed the trial judge's order, protecting the password on Fifth Amendment grounds. The appellate judges ruled that the Foregone Conclusion Doctrine did not apply because the State did not show "reasonable particularity."

Given that two Florida appellate courts have made different rulings, this question will likely go to the Florida Supreme Court at some point. The Court in *G.A.Q.L.* openly disagreed with Florida's Second District Court of Appeal and cited a U.S. 11th Circuit Court of Appeals case that found that the privilege against compelled decryption applies unless the government can describe the incriminating files that are on the device with reasonable particularity (*In Re Grand Jury Subpoena*, 2012).

There are other cases that have resulted in conflicting decisions, showing that there is no clear precedent, among them:

1. *U.S. v. Fricosu* (2012): Citing the All Writs Act, ordered the defendant to supply an unencrypted copy of an encrypted hard drive for which the Government had a search warrant.

2. *U.S. v. Apple MacPro Computer* (2017): Found that compelled decryption did not violate prior decisional law and did not violate Fifth Amendment privilege against self-incrimination.

3. *U.S. v. Spencer* (2018): Held that the appropriate test to determine whether the Foregone Conclusion Doctrine applied was whether the government could show that it was a foregone conclusion that the defendant could decrypt the devices; if so, it allowed compelled decryption.

4. *Seo v. State* (2018): Found that ordering the defendant to unlock a mobile phone was a violation of Fifth Amendment protections against self-incrimination, largely because of the unlimited nature of the search warrant and the fact that the device is an intimate record of a

person's thoughts and actions. The ruling was upheld by the Indiana Supreme Court in 2020 (Lee, 2020; *Seo v. State*, 2020).

It seems that inconsistencies at the Federal level (e.g., *Boucher*, in the U.S. 2nd Circuit, conflicts with *In Re Grand Jury Subpoena*, decided in the U.S. 11th Circuit) suggest that this issue has to eventually be adjudicated by the U.S. Supreme Court. One could argue that the Supreme Court has already missed one opportunity to address this question. The defendant in *Commonwealth v. Jones* (2019) filed a writ of certiorari with the Court in 2019 (Reidy & Nathanson, 2019). The specific questions in the writ were:

Does the Fifth Amendment's act of production doctrine apply to compelled decryption? If so, what does the foregone conclusion exception to the act of production doctrine require the government to show before an order to compel decryption can issue? (Reidy & Nathanson, p. i)

Public defenders in Massachusetts filed an *amicus curiae* brief arguing that *Fisher's* ruling regarding the Act of Production Doctrine should not be applied to compelled decryption (Rangaviz, 2019). The Supreme Court declined to hear the case as they denied certiorari (U.S. Supreme Court, 2019).

4.2 Product and Encryption Backdoors

In December 2015, a mass shooting in San Bernardino, California resulted in 14 people being killed and an additional 21 people wounded. The shooters – a married couple – were both killed in a shootout with police. According to FBI investigators, the couple were lone operator terrorists; "homegrown violent extremists" radicalized over several years of consuming "poison on the Internet" and inspired by foreign terrorist groups committed to jihadism and martyrdom, yet not directed by any particular group (Schmidt & Pérez-Peña, 2015).

The FBI believed that access to the iPhone 5C found in the couple's vehicle would advance their investigation. As iPhone encryption has evolved, law enforcement has requested assistance from Apple many times to retrieve information so as to advance criminal investigations. When Apple complied, it employed existing capabilities to access the devices (Cohen & Park, 2018; Sacharoff, 2018).

In 2016, the Court issued an order requiring a custom operating system be created and installed by Apple without unlocking or otherwise changing the data on the phone (*In re Apple AWA Order*, 2016). What was new in this request was that Apple was asked to develop a new capability to break the advanced security features found in Apple's devices. The basis of the FBI's request to Apple was the All Writs Act of 1789 that allows the government to issue all necessary and appropriate orders in the furtherance of their rightful duties (*In re Apple AWA Application*, 2016). Apple opposed the order on the grounds that it was unlawful and unconstitutional because it essentially conscripted Apple into writing hacking code for the government. Further, they argued that if the order was granted, it would undermine the security of all Apple devices and set a dangerous precedent for future cases (Cohen & Park, 2018; EPIC, n.d.a; *In re Apple Motion to Vacate*, 2016). Subsequently, the FBI found another way into the phone and the matter was dropped (Blum, 2018; Cardozo & Crocker, 2018).

In December 2019, conflicts between the government and Apple resurfaced after a terrorist shooting at Naval Air Station Pensacola (Florida). A member of the Saudi Arabian military in flight training at the air station, later found to have ties with al Qaeda, killed three people and wounded eight others with a handgun before being killed by responding

authorities. Law enforcement wanted to gain access to two of the assailant's phones, an iPhone 5 and iPhone 7. Attorney General William Barr requested Apple's assistance in unlocking the phones and Apple, as in the past, refused the government's request. A.G. Barr was very public in his displeasure that Apple would not assist in this case while Apple made it clear that they had assisted the government in substantive ways, including responding rapidly to their requests and turning over several terabytes of data; Apple merely would not unlock the phones (Feiner, 2020; Lucas, 2020). Eventually, the FBI was able to break into the phones and although they opined that Apple's assistance earlier on would have been helpful, they did not address what new type of information was recovered (Brewster, 2020).

In early 2020, the U.S. Senate introduced the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act of 2020. While the umbrella mission "To establish a National Commission on Online Child Sexual Exploitation Prevention..." is noble, the Trump Administration's publicly stated rationale is because child predators use virtually unbreakable encryption (S.3398, 2020). Of course, so do terrorists and criminals, as well as journalists, political activists, victims of domestic abuse, and other ordinary citizens. While the EARN IT Act does not specifically address encryption, it provides a clear path for the government to force content platforms to eliminate its use (Newman, 2020; Pfefferkorn, 2020).

Section 230 of the Communications Decency Act (CDA) holds Internet social media services, such as Facebook and Twitter, immune from liability for the content on their unmoderated platforms. Thus, if Party A defames Party B on Facebook or Twitter, Party B can sue Party A but cannot sue Facebook or Twitter (47 U.S. Code §?230, 1996). Without Section 230 protections, it is unlikely that social media platforms would exist as they do today (for good or for bad).

The EARN IT Act would remove Section 230 immunity unless social media and other content-hosting platforms comply with a set of guidelines that would be created by an unelected National Commission and could be changed unilaterally at the whim of the U.S. Attorney General. Furthermore, these guidelines are not laws or rules that go through any legislative or formal rulemaking process, although compliance with them provides immunity to the provider (Pfefferkorn, 2020). Clearly, this approach provides a way to incent – or coerce – platforms to do what the Government wants them to do (Cope, Mackey, & Crocker, 2020).

A threat to the use of end-to-end encryption is not explicit in the EARN IT Act; in fact, the only mention of the word "cryptography" is to require that two members of the National Commission be knowledgeable about the subject (S.3398, 2020). But the potential is there for the commission to decide to limit the immunity of a platform that employs end-to-end encryption (Pfefferkorn, 2020). It might also require content providers to examine the content being posted, which would not only bypass the use of encryption but would also make the content provider an agent of the state without a search warrant (Cope et al., 2020). At the time of this paper's submission, the bill is under consideration by the Senate (Ng, 2020).

5. CONCLUSION

Even before the shooting in Pensacola, the Apple-FBI conflict had re-energized the debate about the government's need and ability to get past strong encryption. Once again, discussion started about requiring manufacturers to install backdoors in all encryption products or on ways to ban end-to-end encryption. While this is an idea that might

sound good on paper – as it did two decades earlier – it is impossible to implement cryptographic backdoors without weakening the overall security of any product (Abelson et al., 2015). Many practical issues crop up, as well, including (Claburn, 2019):

1. Who determines who the Good Guys are that get access to the backdoor features?
2. How would use of the backdoor be controlled?
3. How would access to the backdoor ever be rescinded?

But is this not the same idea that the government posed – and the marketplace rejected – in the 1990s with Capstone (IEEE, 2018; Stepanovich & Karanicolas, 2018; Young & Yung, 1996)? And, yet, it seems to remain an attractive idea to governments; as recently as June 2019, senior members of the Trump administration were exploring potential legislation to crack down on end-to-end encryption (Abel, 2019; Claburn, 2019). Indeed, U.S. Attorney General William Barr and officials in Australia and the U.K. have warned high-tech companies that continued use of strong end-to-end encryption could result in stronger regulations and laws limiting such use ("Attorney General", 2019). Interestingly, the European Union Agency for Cybersecurity (ENISA) and Europol released a joint statement in 2016 calling for mechanisms to circumvent commercial encryption methods although they acknowledged that weakened cryptography was not the correct forward path ("On lawful", 2016).

A cryptographic backdoor is a slight variant on *kleptography*, the "...study of stealing information securely and subliminally" (Young & Yung, 1997, p. 63). Unlike a backdoor that weakens a crypto algorithm, kleptography refers to an attack on a cryptosystem from within. Consider this example: Imagine a trusted, black box cryptosystem that generates PKC key pairs. Presumably, the private key cannot be derived from the widely-distributed public key. Suppose that a trapdoor function – called a Secretly Embedded Trapdoor with Universal Protection (SETUP) – is embedded into the cryptosystem that allowed an attacker to access or derive the private key from the public key by weakening the key generation process (Esslinger, 2013; Young & Yung, 1996, 1997). For a practical application of kleptography, consider Edwards Snowden's revelation in 2013 that the NSA deliberately weakened NIST pseudo-random number generator (PRNG) standards, the methods at the very heart of generating secret keys and public key pairs (Zetter, 2013).

This paper poses several questions about reconciling personal privacy with the legitimate needs of the state to conduct investigations. This paper is not intended to answer those questions but to inform the debate. Other related questions might include:

1. Were any of us – as citizens and consumers – ever asked what we wanted, in terms of strong encryption?
2. Is the need for an individual's personal privacy superior to the State's need to investigate crimes?
3. Do we alter the government's duty to provide security with the implementation of processes that could block tools used to reach that objective?
4. Is the subjective expectation of privacy when using encryption so absolute that it meets the "objectively reasonable" test? In particular, does society agree?
5. How did we manage for the last 230 years without this level of protection from the State?

6. Who gave Apple, Google, et al. the right to have unilaterally made the decision about use of strong cryptography without an informed debate?

7. How do we resolve conflicts between the protections of two amendments?

The evolution of technology has always moved faster than the legislative process and the fact that both use a different vernacular does not help in the mutual understanding necessary for the implementation of good laws and regulations (Kessler, 1999). Society, however, cannot address these questions if we are not having the discussion. We cannot move forward toward any type of solution if the various stakeholders continue to hold on to decades-old arguments; our way of thinking about this topic must evolve since neither technology nor the law can afford to stand still.

In June 2020, the Lawful Access to Encrypted Data (LAED) Act was introduced in the U.S. Senate (Bradbury, 2020; Committee on the Judiciary, 2020; Franceschi-Bicchierai, 2020; S.4051, 2020). Legislators are again insisting that technology companies insert cryptographic backdoors into their products and requires similar backdoors in any platform supporting end-to-end encryption, so that they can comply with search warrants. The debate continues.

6. REFERENCES

1. 47 U.S. Code §230. Protection for private blocking and screening of offensive material. (1996, February). U.S. Code, Title 47. Telecommunications, Chapter 5. Wire or Radio Communication, Subchapter II. Common Carriers, Part I. Common Carrier Regulation. Retrieved from https://www.law.cornell.edu/uscode/text/47/230

2. Abel, R. (2019, July 1). Cellebrite Claims it Can Crack any iPhone or Android, Trump Admins Weigh Encryption Ban. *SC Magazine.* Retrieved from https://www.scmagazine.com/encryption-data-security/isreali-data-extraction-firm-cellebrite-announced-the-ability-to-break-into-any-iphone-or-android-device-for-law-enforcement-agencies-as-feds-weigh-banning-tough-encryption/

3. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M., & Weitzner, D.J. (2015, July 6). *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications.* MIT Computer Science and Artificial Intelligence Laboratory Technical Report (MIT-CSAIL-TR-2015-026). Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

4. Apple Inc. (2003, June 23). Apple Previews Mac OS X "Panther." *Press release.* Retrieved from https://www.apple.com/newsroom/2003/06/23Apple-Previews-Mac-OS-X-Panther/

5. Apple Inc. (2018, November 30). Use FileVault to Encrypt the Startup Disk on Your Mac. Retrieved from https://support.apple.com/en-us/HT204837

6. Armerding, T. (2017, March 8). Comey: Strong Encryption "Shatters" Privacy-Security Bargain. *CSO.* Retrieved from https://www.csoonline.com/article/3178299/comey-strong-encryption-shatters-privacy-security-bargain.html

7. Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security. (2019, July 23). Remarks as prepared for delivery, U.S. Department of Justice. Retrieved from https://www.justice.gov/opa/speech/ attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber

8. Blaze, M. (1994, August 20). Protocol Failure in the Escrowed Encryption Standard. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pp. 59–67. Retrieved from http://www.mattblaze.org/papers/eesproto.pdf

9. Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E., & Wiener, M. (1996, January). Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists. Retrieved from https://www.schneier.com/academic/paperfiles/paper-keylength.pdf

10. Blum, S. (2018, October 25). Apple Just Made Its Phones Impossible For Police to Hack. *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/ technology/security /a24219241/apple-greykey-ios12-police-hacking/

11. Bradbury, D. (2020, July 8). LAED Act Poses Direct Threat to End-to-End Encryption. *infosecurity*. Retrieved from https://www.infosecurity-magazine.com/infosec/laed-act-threat-encryption/

12. Brewster, T. (2020, May 19). FBI Hacks iPhones in Pensacola Terrorist Shooting Case, But the War With Apple Goes On. *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2020/05/18/feds-hack-iphones-in-pensacola-case-apple-not-needed-after-all/#1f50e57575e9

13. Cardozo, N., & Crocker, A. (2018, April 2). The FBI Could Have Gotten Into the San Bernardino Shooter's iPhone, But Leadership Didn't Say That. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say

14. Claburn, T. (2019, December 10). Americans Should Have Strong Privacy-Protecting Encryption... That the Feds and Cops can Break, say Senators. *The Register*. Retrieved from https://www.theregister.co.uk/2019/12/10/us_congress_encryption_backdoor_hearings/

15. Clinton, B. (1996, November 15). *Executive Order (EO) 13026: Administration of Export Controls on Encryption Products*. Homeland Security Digital Library. Retrieved from https://www.hsdl.org /?abstract&did=799501

16. Cohen, A., & Park, S. (2018, Fall). Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries. *Harvard Journal of Law & Technology*, *32*(1), 169-234. Retrieved from https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech169.pdf

17. *Commonwealth v. Gelfgatt* (468 Mass 512, 2014). Retrieved from https://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html

18. *Commonwealth v. Jones* (Mass SJC-12564, 481 Mass. 540, 552 n.14, 2019). Retrieved from https://cases.justia.com/massachusetts/supreme-court/2019-sjc-12564.pdf

19. Cope, S., Mackey, A., & Crocker, A. (2020, March 31). The EARN IT Act Violates the Constitution. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/deeplinks/2020/03/earn-it-act-violates-constitution

20. Crypto Museum. (2018, November 25). Clipper Chip. Retrieved from https://www.cryptomuseum.com /crypto/usa/-clipper.htm

21. Diffie, W., & Hellman, M.E. (1976, November). New Directions in Cryptography. *IEEE Transactions on Information Theory, IT-22*(6), 644-654. Retrieved from https://ee.stanford.edu/~hellman/publications/24.pdf

22. *Doe v. U.S.* (487 U.S. 201, 210, 1988). Retrieved from https://supreme.justia.com/cases/federal/us/487/201/

23. Electronic Communications Privacy Act (ECPA) of 1986 (18 U.S.C. §§ 2510-2523). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

24. Electronic Frontier Foundation. (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design.* Sebastopol, CA: O'Reilly & Associates.

25. Electronic Privacy Information Center (EPIC). (n.d.a). Apple v. FBI. Retrieved from https://epic.org /amicus/crypto/apple/

26. Electronic Privacy Information Center (EPIC). (n.d.b). The Clipper Chip. Retrieved from https://www.epic.org/crypto/clipper/

27. Esslinger, B. (2013, February 20). The Dark Side of Cryptography: Kleptography in Black-Box Implementations (P. Vacek, Trans.). *Info Security.* Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-dark-side-of-cryptography-kleptography-in/

28. Feiner, L. (2020, January 14). Apple Refuses Government's Request to Unlock Pensacola Shooting Suspect's iPhones. *CNBC.* Retrieved from https://www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html

29. *Fisher v. U.S.* (425 U.S. 391, Case No. 74-18, 1976). Retrieved from https://caselaw.findlaw.com/us-supreme-court/425/391.html and https://supreme.justia.com/cases/federal/us/425/391/

30. Franceschi-Bicchierai, L. (2020, June 24). Republicans Who Don't Understand Encryption Introduce Bill to Break It. *Motherboard.* Retrieved from https://www.vice.com/en_us/article/y3z3z7/republican-encryption-bill-privacy-signal

31. *G.A.Q.L. v. State of Florida* (Case No. 4D18-1811, Fla 4th DCA, 2018). Retrieved from https://www.documentcloud.org/documents/5021228-181811-1704-10242018-09282906-I.html

32. Committee on the Judiciary. (2020, June 23). Graham, Cotton, Blackburn Introduce Balanced Solution

to Bolster National Security, End Use of Warrant-Proof Encryption That Shields Criminal Activity. *U.S. Senate.* Retrieved from https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity

33. Haufler, H. (2003). *Codebreakers' Victory: How the Allied Cryptographers Won World War II.* New York: New American Library.

34. IEEE. (2018, June 24). In Support of Strong Encryption. *IEEE Position Statement.* Retrieved from http://globalpolicy.ieee.org/wp-content/uploads/2018/06/IEEE18006.pdf

35. *In re Apple AWA Application.* (ED No. 15-0451M, C.D. Cal, 2016). Retrieved from https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWA-Application.pdf

36. *In re Apple AWA Order.* (No. ED 15-0451M, C.D. Cal, 2016). Retrieved from https://epic.org/amicus/crypto/apple/In-re-Apple-AWA-Order.pdf

37. *In re Apple Motion to Vacate.* (ED No. CM 16-10 (SP), C.D. Cal, 2016). Retrieved from https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf

38. *In Re Grand Jury Subpoena.* (670 F.3rd 1335, 11th Cir. 2012). Retrieved from https://www.courtlistener.com/opinion/624132/in-re-grand-jury-subpoena-duces-tecum/

39. *In re Search Warrant Application* (279 F. Supp. 3d 800, 805–06, N.D. Ill. 2017). Retrieved from https://www.leagle.com/decision/infdco20171011995

40. *In the Matter of the Search of a Residence in Aptos, California 95003.* (Case No. 17-mj-70656-JSC-1, 2018 WL 1400401, N.D. Cal, 2018). Retrieved from https://www.leagle.com/decision/infdco20180321a43

41. Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet,* revised ed. New York: Scribner.

42. *Katz v. U.S.* (389 U.S. 347, 88 S.Ct. 507, 19 L.Ed. 2d 576, 1967). Retrieved from https://supreme.justia.com/cases/federal/us/389/347/case.html

43. Kerckhoffs, A. (1883a, January). La Cryptographie Militaire. *Journal des sciences militaires, 9,* 5-38.

44. Kerckhoffs, A. (1883b, February). La Cryptographie Militaire. *Journal des sciences militaires, 9,* 161-191.

45. Kerr, O. (2018, April 29). Suspect Can Be Compelled to Decrypt Devices If Government Proves He Has The Ability To Do So, Court Rules. *The Volokh Conspiracy.* Retrieved from https://reason.com /2018/04/29/suspect-can-be-compelled-to-decrypt-devi

46. Kerr, O.S. (2019, March). Compelled Decryption and the Privilege Against Self-Incrimination. *Texas Law Review, 97*(4), 767-799. Retrieved from https://texaslawreview.org/wp-content/uploads/2019/03/Kerr.V97.4.pdf

47. Kessler, G.C. (1999, September). Catch My Drift? Can You Define "Digital Signature" in Non-Technical Terms? The Future of E-Commerce Law May Depend on it. *Information Security Magazine.* Retrieved from https://www.garykessler.net/library/is_language.html

48. Kessler, G.C. (2020, June 1). An Overview of Cryptography. Retrieved from https://www.garykessler.net/library/crypto.html

49. Lee, T.B. (2020, June 24). It's Unconstitutional For Cops to Force Phone Unlocking, Court Rules. *Ars Technica.* Retrieved from https://arstechnica.com/tech-policy/2020/06/indiana-supreme-court-its-unconstitutional-to-force-phone-unlocking/

50. Levy, S. (1999, April). The Open Secret. *WIRED Magazine, 7(??).* Retrieved from http://www.wired.com/wired/archive/7.04/crypto.html

51. Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age.* New York: Viking Press.

52. Lucas, S. (2020, January 13). Apple Said it is Helping in the Pensacola Shooting Investigation, But it Won't Unlock the Shooter's iPhone. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/scottlucas/william-barr-apple-request-unlock-iphones

53. Marks, L. (1998). *Between Silk and Cyanide: A Codemaker's War, 1941-1945.* New York: The Free Press (Simon & Schuster).

54. Meeks, B.N. (1994, September 1). Clipping Clipper: Matt Blaze. *WIRED.* Retrieved from https://www.wired.com/1994/09/clipping-clipper-matt-blaze/

55. Miller, J. (2014, September 19). Google and Apple to Introduce Default Encryption. *BBC News.* Retrieved from https://www.bbc.com/news/technology-29276955

56. Nakashima, E. (2008, January 16). In Child Porn Case, a Digital Dilemma. *Washington Post.* Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663.html

57. National Institute of Standards & Technology (NIST). (2018, October 10). *Cryptographic Standards and Guidelines: AES Development.* Information Technology Laboratory, Computer Security Resource Center. Retrieved from https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

58. Newman, L.H. (2020, March 5). The EARN IT Act is a Sneak Attack on Encryption. *WIRED.* Retrieved from https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/

59. Ng, A. (2020, July 2). Why Your Privacy Could be Threatened by a Bill to Protect Children. *CNET.* Retrieved from https://www.cnet.com/news/why-your-privacy-could-be-threatened-by-a-bill-to-protect-children/

60. *Olmstead v. U.S.* (277 U.S. 438, 19 F. (2d) 842, 848, 850, affirmed, 1928). Retrieved from https://www.law.cornell.edu/supremecourt/text/277/438

61. On Lawful Criminal Investigation That Respects 21st Century Data Protection. (2016, May 20). Europol and ENISA Joint Statement. Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

62. OSXDaily. (n.d.). What is FileVault? FileVault for Mac Explained. Retrieved from http://osxdaily.com /what-is-filevault/

63. Painter, L. (2020, June 22). Complete List of Mac OS X & MacOS Versions. *Macworld.* Retrieved from https://www.macworld.co.uk/feature/mac/mac-os-x-macos-version-code-names-3662757/

64. Pfefferkorn, R. (2020, January 30). The EARN IT Act: How to Ban End-to-End Encryption Without Actually Banning it. *The Center for Internet and Society at Stanford Law School.* Retrieved from https://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it

65. Rangaviz, D.R. (2019, October 22). Brief Of Amicus Curiae Committee For Public Counsel Services In Support Of Petition For A Writ Of Certiorari: Dennis Jones, Petitioner, v. Commonwealth Of Massachusetts, Respondent (No. 19-6275). Retrieved from http://www.supremecourt.gov/DocketPDF/19/19-6275/120068/20191024102615254_Jones%20v.%20Massachusetts%20CPCS%20Amicus%20Brief.pdf

66. Reidy, J.A., & Nathanson, D. (2019, August 7). Petition for a Writ of Certiorari: Dennis Jones, Petitioner v. Commonwealth of Massachusetts, Respondent (No. 19-6275). Supreme Court of the United States. Retrieved from http://www.supremecourt.gov/DocketPDF/19/19-6275/118752/20191010183703372_Jones%20Cert%20Petition%20Final.pdf

67. Rivest, R.L., Shamir, A., & Adleman, L. (1978, February). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126. Retrieved from https://people.csail.mit.edu/rivest/Rsapaper.pdf

68. S.3398. (2020, March 5). EARN IT Act of 2020: A Bill to Establish a National Commission on Online Child Sexual Exploitation Prevention, and for other purposes. *116th Congress (2019-2020).* Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

69. S.4051. (2020, June 23). Lawful Access to Encrypted Data Act. *116th Congress (2019-2020).* Retrieved from https://www.judiciary.senate.gov/download/s4051_-lawful-access-to-encrypted-data-act

70. Sacharoff, L. (2018). Unlocking the Fifth Amendment: Passwords and Encrypted Devices. *Fordham Law Review, 87*(1). Retrieved from https://ir.lawnet.fordham.edu/flr/vol87/iss1/9

71. Schmidt, M.S., & Pérez-Peña, R. (2015, December 4). F.B.I. Treating San Bernardino Attack as Terrorism Case. *The New York Times.* Retrieved from https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html

72. Schneier, B. (2004, October 6). The Legacy of DES. *Schneier on Security.* Retrieved from https://www.schneier.com/blog/archives/2004/10/the_legacy_of_d.html

73. *Seo v. State* (109 N.E.3d 418, 425–31, Ind. Ct. App. 2018). Retrieved from https://www.leagle.com/decision/ininco20180821261

74. *Seo v. State* (Supreme Court Case No. 18S-CR-595, 2020). Retrieved from https://www.eff.org/files/2020/06/23/opinion_issued_reversed_and_rem.pdf

75. Singh, S. (1999). *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography.* New York: Doubleday.

76. *Smith v. Maryland* (442 U.S. 735, 1979). Retrieved from https://supreme.justia.com/cases/federal/us/442/735/

77. *State of Florida v. Stahl* (206 So. 3d 124, 136–37, Fla 2nd DCA, 2016). Retrieved from https://www.leagle.com/decision/inflco20161207102

78. Stepanovich, A., & Karanicolas, M. (2018, March 2). Why An Encryption Backdoor for Just the "Good Guys" Won't Work. *Just Security.* Retrieved from https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

79. Sussman, V. (1995, March 26). Lost in Kafka Territory. *U.S. News & World Report.* Retrieved from https://web.archive.org/web/20130616165334/http://www.usnews.com/usnews/news/articles/950403/archive_010975.htm

80. TrueCrypt. (2015, July 31). TrueCrypt Version History. Retrieved from https://www.truecrypt71a.com/documentation/version-history/

81. TrueCrypt Foundation. (2012, February 7). *TrueCrypt User's Guide*, version 7.1a. Retrieved from https://www.grc.com/misc/truecrypt/ TrueCrypt%20User%20Guide.pdf

82. *U.S. Const. amends. IV, V.*

83. U.S. Department of Commerce. (2000, January 10). *Revisions to Encryption Items.* Bureau of Export Administration, 15 CFR Parts 734, 740, 742, 770, 772, and 774. Retrieved from https://epic.org /crypto/-export_controls/regs_1_00.html

84. U.S. Supreme Court. (2019, October 16). Petition for a Writ of Certiorari Related to Dennis Jones, Petitioner v. Massachusetts (No. 19-6275). Retrieved from https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/19-6275.html

85. *U.S. v. Apple MacPro Computer* (851 F.3d 238, 248 & n.7, 3d Cir. 2017). Retrieved from https://www.leagle.com/decision/infco20170320056

86. *U.S. v. Boucher* (2007 WL 4246473, 2009). Retrieved from http://www.volokh.com/files/Boucher.pdf

87. *U.S. v. Fricosu* (841 F. Supp. 2d 1232, 1237, D. Colo. 2012). Retrieved from https://www.leagle.com/decision/ inadvfdco120925000244

88. *U.S. v. Hubbell* (530 U.S. 27, 2000). Retrieved from https://supreme.justia.com/cases/federal/us/530/27/

89. *U.S. v. Spencer* (No. 17-CR-00259-CRB-1, 2018 WL 1964588, N.D. Cal, 2018). Retrieved from https://orinkerrblog.files.wordpress.com/2018/04/usvspencer.pdf

90. Warren, S., & Brandeis, L. (1890, December 15). The Right to Privacy. *Harvard Law Review, 4*, 193. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

91. Written Testimony for the United States Senate Committee on the Judiciary on Smartphone Encryption and Public Safety. (2019, December 10). Manhattan District Attorney's Office. Retrieved from https://www.manhattanda.org/written-testimony-for-the-united-states-senate-committee-on-the-judiciary-on-smartphone-encryption-and-public-safety/

92. Yardley, H.O. (1931). *The American Black Chamber.* Indianapolis: The Bobbs-Merrill Company.

93. Young, A., & Yung, M. (1996). The Dark Side of Black-Box Cryptography, or: Should We Trust Capstone? In N. Koblitz (Ed.), *Advances in Cryptology – CRYPTO '96: 16th Annual International Cryptology Conference*, Santa Barbara, California, August 18–22 (pp.89-103). New York: Springer. Retrieved from https://www.researchgate.net/publication/225139661_The_Dark_Side_of_Black-Box_Cryptography_or_Should_We_Trust_Capstone

94. Young, A., & Yung, M. (1997). Kleptography: Using Cryptography Against Cryptography. In W. Fumy (Ed.), *Advances in Cryptology - EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques*, Konstanz, Germany, May 11-15 (pp.62-74). New York: Springer-Verlag. Retrieved from https://www.researchgate.net/publication/221348188_Kleptography_Using_Cryptography_Against_Cryptography

95. Zetter, K. (2013, September 24). How a Crypto 'Backdoor' Pitted the Tech World Against the NSA. *Wired Magazine.* Retrieved from https://www.wired.com/2013/09/nsa-backdoor/

96. Zimmermann, P. (n.d.). Philip Zimmermann. Retrieved from https://philzimmermann.com/EN/background/index.html

97. Zimmermann, P. (1999). Why I Wrote PGP. Retrieved from https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

98. Zimmermann, P. (2001, June 5). PGP Marks its 10th Anniversary. Retrieved from http://www.philzimmermann.com/EN/news/PGP_10thAnniversary.html

Privacy issues and the law	Timeline	Issues and events
	2600 BCE	Writing appears
	1900 BCE	Secret writing appears
U.S. Constitution ratified	1789	
Bill of Rights ratified	1791	
"The Right to Privacy"	1890	
	1914-1918	Cryptography in WW I
Olmstead v. U.S.	1928	
	1939-1945	Cryptography in WW II
	1948	Cryptography classified as a munition
Katz v. U.S.	1967	
	1969	Advanced Research Projects Agency Network (ARPANET)
Fisher v. U.S.	1976	PKC concept described
	1977	DES released
	1978	RSA described
Smith v. Maryland	1979	
	1985	National Science Foundation Network (NSFNET)
Electronic Communications Privacy Act	1986	
Doe v. U.S.	1988	
	1991	PGP released on the Internet
		Commercialization of the Internet
	1993	FBI starts Zimmermann investigation
		Capstone program proposed
	1995	Zimmermann receives EFF Pioneer Award
		SSL introduced
	1996	FBI closes Zimmermann investigation
		Capstone project dead
		EO 13026 released
		Blaze et al.: "56-bit keys are dead"
	1997	NIST starts AES process
		"Kleptography" defined
	1998	EFF Deep Crack chip: "DES is dead"
U.S. v. Hubbell	2000	Commerce Dept. reclassifies cryptography
	2001	AES adopted
	2003	FileVault (home directory) released
	2004	TrueCrypt and plausible deniability released
U.S. v. Boucher	2009	
	2011	FileVault 2 (full volume) released
In Re Grand Jury Subpoena U.S. v. Fricosu	2012	
	2013	Snowden revelations about NSA
Commonwealth v. Gelfgatt	2014	Android 5.0 introduces default encryption
		Apple iOS 8 introduces default encryption
	2015	San Bernardino terrorist shooting
State of Florida v. Stahl	2016	FBI versus Apple
U.S. v. Apple MacPro Computer	2017	Crypto backdoors back in public discussion
G.A.Q.L. v. State of Florida	2018	
U.S. v. Spencer		
Seo v. State		
Commonwealth v. Jones	2019	NAS Pensacola terrorist shooting
SCOTUS denies certiorari in Jones		
EARN IT Act introduced in U.S. Senate	2020	
LAED Act introduced in U.S. Senate		
Seo v. State upheld		

Table 1. Timeline

Federal Intelligence Surveillance Court (FISC)

The Foreign Intelligence Surveillance Court (FISC) was established in 1978 with the enactment of the Foreign Intelligence Surveillance Act (FISA). The original act has been amended many times since its original enactment. The make-up of the court and the many of the rules by which it operates are codified in the U.S. Code at 50 U.S.C. §§ 1801-1885c. This specialized Article III court reviews government applications to conduct electronic surveillance for domestic foreign intelligence purposes.

Structure of the Court

The Court itself is seated in Washington D.C., and is currently composed of eleven federal district court judges who have been designated by the Chief Justice of the United States for this additional assignment. No Senate confirmation for this additional duty assignment is required. Each judge on the FISC serves for a maximum of seven years and may not be re-designated. The terms of the judges are staggered in order to ensure the continuity of the Court; one judge is designated by the Chief Justice as the "presiding judge" and handles various administrative duties of the Court, such as assigning matters to the judges of the court. Pursuant to federal statute, the judges must, at all times, represent at least seven of the U.S. judicial circuits. Additionally, three of the judges must reside within 20 miles of the District of Columbia. Typically, each week one of the designated judges sits on the FISC in Washington, on a rotating basis. Most of the Court's work is handled by that duty judge and the support of attorneys and the personnel from the clerk's office. The more complex or time-consuming matters are assigned outside the duty-week system by the presiding judge

Secrecy

The FISC is unique in that, contrary to typical courts of law, much of this court's work is conducted in secret. As the name provides, this court is responsible for reviewing government applications for surveillance and other investigative activities relating to foreign intelligence collection. In addition, orders of the court, including those which entail the court's legal analysis, often contain highly sensitive information. The release of such information could be damaging to national security. Documents which do not contain classified material and those which the FISC has deemed safe for dissemination can be found on the FISC's website at http://www.fisc.uscourts.gov/.

For security reasons, the FISC has its own clerk of court who is responsible for the record keeping, filings, and conventional duties of a court's clerk. All of FISC's staff must possess and maintain security clearances commensurate with their individual responsibilities.

Practice before the Court

Attorneys must be licensed and a member, in good standing, of a U.S. district or circuit court. An exception is made in that an attorney who is employed by and representing the U.S. or any of its agencies in a FISC matter may appear before the Court regardless of federal bar membership. All attorneys appearing before the FISC must have security clearances appropriate to the case and

information involved. Parties other than the government must provide information regarding their security clearances in their initial submissions to the court. The non-government litigants who have the right to challenge a FISC order are individuals and companies who have been ordered to turn over information regarding a particular target.

In June of 2015, both FISC and its court of review were mandated by statute to jointly designate no fewer than five individuals to be eligible to serve as amicus curiae, also known as friends of the court. The duty of the amicus curiae is to assist the court in the consideration of any filing that, in the opinion of the court, presents a novel or significant interpretation of the law. Additionally, amicus curiae may be appointed to provide technical expertise. In order to be considered eligible for designation, a person must be one who possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise to either the FISC or the FISC court of review. Like the attorneys who appear before the courts, amicus curiae must be eligible for access to classified information necessary to participate in matters before the courts, if such access is necessary to participate in the matters in which they may be appointed.

Matters Presented to the Court

All FISA orders are reviewed by this special court. There are four means of requesting relief from the FISC: by application, by certification, by petition and by motion. An application is the most commonly used filing document when the government seeks to conduct domestic foreign surveillance pursuant to federal statutes. The government may also, when targeting non-U.S. persons reasonably believed to be located outside the United States, file a certification. Parties may file petitions with the court when seeking to review a production or non-disclosure order issued by the court or for review of enforcement of a directive. For example, an electronic communications service provider who has received a directive may file a petition to modify or set aside the directive; the government could file a petition to compel compliance with a directive where such compliance has not been forthcoming in accordance with the directive. A party seeking another type of relief must do so by filing a motion. The FISC has jurisdiction to hear applications for, and issue orders authorizing, four traditional FISA activities: electronic surveillance, physical searches, pen/trap surveillance, and compelled production of tangible things. In addition, the FISC has jurisdiction to review the government's targeting and minimization procedures related to programmatic surveillance certified under Section 702 of the FISA Amendments Act of 2008.

Pursuant to statutory authority, the FISC entertains applications submitted by the U.S. government and its agencies for approval of electronic surveillance, physical searches, and other investigative actions conducted for foreign intelligence purposes. In most circumstances, the government submits a proposed application, sometimes referred to as a "read copy," to the FISC no later than seven days prior to the government seeking to have the matter entertained; applications for bulk collection are typically filed more than one week in advance in order to allow for more exacting review using this same process. Upon receipt, someone from the Court's legal staff reviews the application to evaluate whether it meets the legal requirements under the statute. After discussion with the government about the application, a written assessment is prepared by the court's attorney. This assessment is given to the duty judge for the week. The

judge will review both the application and the legal staff's evaluation. A preliminary decision will be made by the judge regarding the course of action to be taken. Possible action include: approval without a hearing; imposing conditions on the approval; seeking additional information; or deciding a hearing is required prior to ruling. The judge's preliminary decision is conveyed to the government which can they proceed by providing additional information, filing a final application, or filing a final application with amendments; the government could also decide not to file a final application after learning the judge intends to deny it.

If the judge decides to deny the application, the judge must immediately prepare a written order denoting each of the reasons for the denial. In practice, the methodology of the process of application and review is similar to that utilized by other federal courts in their consideration of applications for wiretap orders under Title III of the Omnibus Crime Control and Safe Streets Act, codified at 18 U.S.C. §§ 2510-2522.

The process for addressing what is commonly referred to as Section 702 applications, see 50 U.S.C. § 1881a, the process differs, but is based in large part on the statutory requirements set forth in the Code. The statute requires that, prior to implementation of such an authorization, both the Attorney General and the Director of National Intelligence must provide the FISC with a written certification. The court the reviews the certification not later than 30 days after the date upon which the certification is submitted. Similar to the other process, a read copy is submitted and reviewed by court staff, recommendations for changes are made

Ex Parte Communications

In addition to being conducted in secret, most of the Court's work is also conducted *ex parte*, meaning with only one side presenting information to the court. This aspect of the court is both required by statute and based upon the need to protect classified national security information. As part of the review process, the court's attorney will often have multiple conversations with the government's attorney to seek additional information and/or discuss concerns with the application. As stated above, this is similar to the process employed in the federal courts when addressing applications for wiretap orders. A typical interaction would include telephone conversations on secure lines wherein the court staff ask the government questions regarding the legal and factual elements of the application or submission. Additionally, the FISC, pursuant to statute and the procedural rules, holds hearings in which the judge assesses the information needed to make a fair determination on the matter at hand. Hearing are attended by, at a minimum, the attorney from the Department of Justice who prepared the application and a fact witness from the agency seeking the authorization of the court. Topics of the hearings will generally include the court seeking additional information on additional facts to justify the government's belief that the application is warranted, additional information on minimization procedures, any prior implementation of a court order, and/or information about a novel issue of law or new technology. It is standard procedure for the court to seek such information in a fair majority of cases.

Court Orders

If the FISC judge determines that the final application has met all the statutory requirements and should be granted, the judge must issue an order approving the surveillance or search. Pursuant to statute, the order must describe the target, the information sought, the means of acquiring the information, and the period of time the order covers.

If a judge denied a final application of the government, that judge must provide a written statement providing the reasons for its ruling. The author of an opinion, order or other decision may, either on their own or pursuant to a party, request the publication of the document. Upon such a request, the other judges are consulted. Prior to publication, the FISC may direct the Executive Branch to review the document and redact it as necessary to ensure that properly classified material is protected. Since the enactment of the FREEDOM Act, the Director of National Intelligence (DNI) is responsible for reviewing each FISC order or opinion to determine whether it "includes a significant construction or interpretation of any provision of law." If so, it must be made public "to greatest extent practicable." When necessary to protect national security, however, the office of the DNI may release a summary of the order or opinion.

En Banc Proceedings

Pursuant to statute, the FISC may sit *en banc*, wherein the entire FISC membership sits to hear a case. The court only orders or grants such a determination where it deems it necessary to secure or maintain the uniformity of the court's decisions, or where the case presents an issue of exceptional importance.

Foreign Intelligence Surveillance Court of Review

The Foreign Intelligence Surveillance Court of Review (FISCR) was established in 1978 in the same bill which created the FISC. As the FISC does, the review court sits in Washington D.C. The review court is composed of three federal district court or appeals court judges who are designated to sit in that capacity by the Chief Justice of the United States Supreme Court. The purposed of this court is to review the decisions of the Foreign Intelligence Surveillance Court, much in the same way the federal circuit courts of appeal review decisions of the federal district court.

The clerk which handles the matters of the FISC also takes care of the review court's filings and docket. In order to appeal a FISC decision to the review court, a party must file a petition of review with the clerk no later than 30 days after the entry of the decision or order for which review is sought. If necessary, the U.S. Supreme Court can, in certain circumstances, review FISCR decisions.

Ann Phillips

Further Reading

50 U.S.C. §§ 1801-1885c

https://fas.org/irp/agency/doj/fisa/#rept

http://www.fisc.uscourts.gov/

Reagan, Robert Timothy. "Foreign Intelligence Surveillance Act Litigation." Jurisdiction of the Federal Courts | Federal Judicial Center, 26 Sept. 2016, www.fjc.gov/content/305810/foreign-intelligence-surveillance-act-litigation.

Nolan, Andrew and Thompson II, Richard M., CRS Report R43362, Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes. 16 Jan. 2014. https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2235&context=key_workplace

See Also

Foreign Intelligence Surveillance Act of 1978

History

The Foreign Intelligence Surveillance Act (FISA or the Act) was signed into law by President Jimmy Carter on October 25, 1978. The catalyst for the Act was of a series of revelations starting in the 1950s and continuing through the 1970s regarding various warrantless surveillance activities of federal and state law enforcement agencies, national security organizations, and military intelligence. The multiple disclosures of abuses led to congressional hearings, often referred to as the Church Committee hearings, named after Senator Frank Church, who headed one of the Senate committees conducting the investigations. Also, the United States Supreme Court weighed in on domestic terrorist activity in United States v. U.S. District Court, 407 U.S. 297 (1972). This case is often referred to as the Keith case, so after Judge Damon Keith, the federal district judge in the lower court. It remains an important case addressing the extent to which the President, acting in the interest of national security, may authorize warrantless electronic surveillance of persons within the United States.

The Code

FISA is codified, as amended, at 50 U.S.C. §§ 1801-1885c. The Act is comprised of seven subchapters, each addressing a particular aspect of foreign intelligence surveillance. The subchapters include electronic surveillance (§§ 1801-1813); physical searches (§§ 1821-1829); pen registers and trap and trace devices for foreign intelligence purposes (§§ 1841-1846); access to certain business records for foreign intelligence purposes (§§ 1861-1864); oversight (§§ 1871-1874); additional procedures regarding certain persons outside the United States (§§ 1881-1881g); and protection of persons assisting the government (1885-1885c). Additionally, the Act created the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review to oversee requests for surveillance warrants by federal law enforcement and intelligence agencies.

The intent underpinning FISA was to allow the continued collection of national security intelligence while preserving the civil liberties granted by the Constitution. Congress recognized the need to distinguish foreign intelligence gathering from surveillance for law enforcement purposes. Where many people get confused is by the term "foreign." As relating to this Act, the term "foreign" generally refers to the target rather than the location. Electronic surveillance and physical searches of an entity that does not fall within the definition of a "foreign power" or an "agent of a foreign power" are governed by Title III and Federal Rule of Criminal Procedure 41.

In broad terms, the Act gives each branch of our national government some role in regulating foreign intelligence. The Act establishes the process for the government (executive branch) to obtain surveillance warrants for gathering intelligence within the U.S. for foreign intelligence and/or foreign counterintelligence, as well as creating the court system (judicial branch) with judicial review of the process. Additional oversight rests with Congress (legislative branch).

Amendments

The Act has been amended numerous times since its enactment. Significant amendments include the USA PATRIOT Act; Terrorist Surveillance Act of 2006; Protect America Act of 2007; FISA Amendments Act of 2008; FISA Amendments Act Reauthorization Act of 2012; USA FREEDOM Act of 2015; FISA Amendments Reauthorization Act of 2017. An additional amendment, the USA FREEDOM Reauthorization Act of 2020, has been passed by both houses of Congress and is currently in the process of being reconciled. If the 2020 amendment becomes law, it will reauthorize FISA provisions relating to intelligence gathering and amend FISA-related provisions; the amendments would expire December 1, 2023.

Ann Phillips

Further Reading

50 U.S.C. ch.36

https://fas.org/irp/agency/doj/fisa/

https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286

Tallman, Richard C. and Culbertson, Tania M., *2019 James R. Browning Distinguished Lecture in Law, "Holding the Delicate Balance Steady and True." The History of FISA's Grand Bargain*, 80 Mont. L. Rev. 137 (2019).

United States v. U.S. District Court, 407 U.S. 297 (1972)

Q 38

Course Outlines

COURSE PROPOSAL

Viewing: BA 225 : Business Law

Primary Campus
Daytona Beach

DB College
Daytona College of Business

DB Department
Management, Marketing and Operations Department

Course Level
Undergraduate

Course Prefix
BA

Course Number
225

Course Title
Business Law

Description

Course Description
This course is an overview of the law as it pertains to business relations and business transactions. Areas covered include procedure; torts; criminal law and procedure; constitutional law; administrative law; contracts; agency; real property; personal property; wills; trusts and estates; insurance law; employment law; commercial transactions; secured transactions; creditor/debtor law; and negotiable instruments. Areas of the law applicable to the aviation industry will also be covered.

Hours
Credit Hours
3

Components
Lecture

Goals

Course Goals
This course is designed to acquaint the student with the legal setting of business, as well as its relationship to one's personal affairs, in a meaningful, accurate and interesting manner. It contributes to the overall objectives of the above-cited management degree programs and should be taken prior to enrollment in the 400-level courses.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Recognize the role and importance of the legal environment of business and how law affects both business and society in conducting commercial transactions.
2	Discuss the nature and role of jurisdiction over subject matter, property, and locations.
3	Explain the role, nature, history, and operational functions of various federal and state courts in the American Jurisprudence system.

4	Describe the major differences existing between private wrongs and public crimes as they affect the business community.
5	Recognize the nature, formation, and classification of contracts and explain the role of the basic elements for a legally valid contract to exist.
6	Assess the legal problems of genuineness of assent and what condition must prevail in order for a contractual offer to be null and void relative to absence of genuineness.
7	Explain how the statute of frauds rule functions and the affects of the parol evidence rule relative to written contracts required under statute of frauds rule.
8	Explain the rights of assignment, delegation, and third party beneficiary contracts as they affect business including remedies available for breach and their discharge.
9	Analyze commercial problems dealing with sales contracts from the standpoint of issues, causes, and potential solutions when performance is incomplete and a breach of contract develops.
10	Explain the role and operational characteristics of warranty of titles, express warranty, warranty of merchantability and fitness for a particular purpose and implied warranty dealing with prior course of dealing including role of product liability for manufacturers.
11	Describe the role of personal property relative to property rights, and the elements of bailment and how they function in different bailment situations.

Learning Outcomes - University MCO

	Outcome
1	Recognize the role and importance of the legal environment of business and how law affects both business and society in conducting commercial transactions.
2	Discuss the nature and role of jurisdiction over subject matter, property, and locations.
3	Explain the role, nature, history, and operational functions of various federal and state courts in the American Jurisprudence system.
4	Describe the major differences existing between private wrongs and public crimes as they affect the business community.
5	Recognize the nature, formation, and classification of contracts and explain the role of the basic elements for a legally valid contract to exist.
6	Assess the legal problems of genuineness of assent and what condition must prevail in order for a contractual offer to be null and void relative to absence of genuineness.
7	Explain how the statute of frauds rule functions and the affects of the parol evidence rule relative to written contracts required under statute of frauds rule.
8	Explain the rights of assignment, delegation, and third party beneficiary contracts as they affect business including remedies available for breach and their discharge.
9	Analyze commercial problems dealing with sales contracts from the standpoint of issues, causes, and potential solutions when performance is incomplete and a breach of contract develops.
10	Explain the role and operational characteristics of warranty of titles, express warranty, warranty of merchantability and fitness for a particular purpose and implied warranty dealing with prior course of dealing including role of product liability for manufacturers.
11	Describe the role of personal property relative to property rights, and the elements of bailment and how they function in different bailment situations.

Proposal Details

Cost

Impact

Additional Information

Key: 703

COURSE PROPOSAL

Viewing: CYB 465 : Cybercrime and Cyberlaw

Primary Campus
Daytona Beach

DB College
Daytona College of Arts & Sciences

DB Department
Security Studies and International Affairs Dept

Course Level
Undergraduate

Course Prefix
CYB

Course Number
465

Course Title
Cybercrime and Cyberlaw

Description

Course Description
Types of criminal behavior in cyberspace, such as identify theft, white collar crimes, fraud, child sexual exploitation, intellectual property theft, and online scams. Laws governing cyberspace, defining criminal activity and guiding law enforcement investigations; U.S. decisional law guiding search and seizure of digital devices and information; international laws related to computer crime and privacy.

Hours
Credit Hours
3

Components
Lecture

Prerequisites - Enforced
CYB 235;

Goals

Course Goals
This course introduces students to different types of crimes that can be perpetrated on the Internet. It will demonstrate how digital devices can be the instrument, record keeper, or victim of criminal activity, and provides an understanding of the legal protections and guidelines in cyberspace.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Explain what cybercrime is and the scope of the problem in today's society.
2	Characterize different ways in which individuals attack cyber systems and differentiate between the motives of different types of hackers.

3	Differentiate different ways in which cyber-based financial fraud and identity theft can be perpetrated and the ways in which individuals and organizations can stay (relatively) safe.
4	Examine the many ways in which child sexual exploitation has been enabled by the Internet and the societal and law enforcement response to these types of crimes.
5	Outline the methods used by a cyber stalker or cyberbully.
6	Examine the different ways in which intellectual property can be stolen in cyberspace, the cost to society, and the ethical issues of "information wants to be free".
7	Construct a typology of those that perpetrate cyber-based crimes.
8	Examine the laws in the U.S. that apply to cybercrime and that provide guidance to ISPs, organizations, law enforcement, and the courts.
9	Apply U.S. laws as they pertain to privacy of information in cyberspace, and the seizure and search of digital devices.
10	Identify major components of international law that applies to cyberspace and privacy.

Learning Outcomes - University MCO

	Outcome
1	Explain what cybercrime is and the scope of the problem in today's society.
2	Characterize different ways in which individuals attack cyber systems and differentiate between the motives of different types of hackers.
3	Differentiate different ways in which cyber-based financial fraud and identity theft can be perpetrated and the ways in which individuals and organizations can stay (relatively) safe.
4	Examine the many ways in which child sexual exploitation has been enabled by the Internet and the societal and law enforcement response to these types of crimes.
5	Outline the methods used by a cyber stalker or cyberbully.
6	Examine the different ways in which intellectual property can be stolen in cyberspace, the cost to society, and the ethical issues of "information wants to be free".
7	Construct a typology of those that perpetrate cyber-based crimes.
8	Examine the laws in the U.S. that apply to cybercrime and that provide guidance to ISPs, organizations, law enforcement, and the courts.
9	Apply U.S. laws as they pertain to privacy of information in cyberspace, and the seizure and search of digital devices.
10	Identify major components of international law that applies to cyberspace and privacy.

Proposal Details

Cost

Impact

Additional Information

Key: 1605

HSI 110: INTRODUCTION TO HOMELAND SECURITY

Viewing: HSI 110 : Introduction to Homeland Security

Formerly known as: HS 110

Last approved: Wed, 16 Feb 2022 09:00:41 GMT

Last edit: Tue, 15 Feb 2022 15:21:36 GMT

Proposer(s) Information

First Name	Last Name	Title	Email
Ann	Phillips	Program Coordinator for HS	philla15@erau.edu

Primary Campus
Daytona Beach

Anticipated effective date for your proposal:
05/01/2022

DB College
Daytona College of Arts & Sciences

DB Department
Security Studies and International Affairs Dept

Course Level
Undergraduate

Course Prefix
HSI

Course Number
110

Course Title
Introduction to Homeland Security

Is this a Gen Ed course?
No

Detailed Description of Proposed Change
Change prefix to HSI
Update course description, goals, and learning outcomes to comply with new AP05 guidance.

Description

Course Description
Introduce the multidisciplinary approach to protecting and defending America. Knowledge domains of intelligence, emergency management, law and policy, critical infrastructure and resilience, strategic planning and decision-making, terrorism, cyberspace, human and environmental security, risk analysis and management, and professionalism.

Hours

Credit Hours
3

Components
Lecture

Lecture Hours per week
3

Teaching Disciplines

Civics / Computer Science / Computer Technology / Criminal Justice / Criminology / Cyber Security / Economics / Emergency Management / Foreign Affairs / Foreign Services / Forensics / Geography / Government / Health Services Research / History / Homeland Security / Intelligence Studies / International Affairs / International Relations/ Law / Military Technologies / National Security / Political Science / Politics / Population Health / Public Health / Public Policy / Public Policy Administration / Safety Management / Security / Security Management / Security Services / Social Science / Sociology / Strategic Studies / Terrorism Studies / Transportation Logistics

Related Disciplines

Business Administration / Law Enforcement /

Goals

Course Goals

To introduce students to the enterprise, infrastructure, risks, goals, and challenges of homeland security and intelligence in the United States today as well as the structure and opportunities of the homeland security and intelligence program at Embry Riddle Aeronautical University (ERAU).

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Illustrate the main functions and components of the U.S. Department of Homeland Security.
2	Identify the structure, laws, acts, policy, and regulatory authority for homeland security and intelligence.
3	Summarize the domains that characterize homeland security such as emergency management, law and policy, critical infrastructure and resilience, strategic planning and decision-making, terrorism, cyberspace, human and environmental security, risk analysis, and professionalism.
4	Describe the intelligence function and relationship to homeland security.

Learning Outcomes - University MCO

	Outcome
1	Illustrate the main functions and components of the US Department of Homeland Security.
2	Identify the structure, laws, acts, policy, and regulatory authority for homeland security and intelligence.
3	Summarize the domains that characterize homeland security such as emergency management, law and policy, critical infrastructure and resilience, strategic planning and decision-making, terrorism, cyberspace, human and environmental security, risk analysis, and professionalism.
4	Describe the intelligence function and relationship to homeland security.

Proposal Details

Describe the need and rationale for the modifications proposed.

Updates prefix to reflect the new degree and program title

Brings current the course description, goals, and learning outcomes to comply with new AP05 guidance

What programs accept this course as an elective?

Affected Programs
DBSSO - B.S. in Space Operations

Cost

Provide a detailed cost estimate for the proposed course.

No costs will be incurred with this proposal

Impact

Specify which programs will be affected by this proposed change.

Affected Programs
DBSHSI - B.S. in Homeland Security and Intelligence
DMHOMESEC - Homeland Security
DBSCS - B.S. in Computer Science
DBSSO - B.S. in Space Operations

Specify effect on facilities and equipment.

There will be no impact on facilities

Additional Information

Key: 2373

History

1. Feb 16, 2022 by Ann Phillips (philla15)

HS 280: PROFESSIONAL SKILLS IN HOMELAND SECURITY

Course Deactivation Proposal

Viewing: HS 280 : Professional Skills in Homeland Security

Last approved: Fri, 04 Mar 2022 09:00:41 GMT

Last edit: Wed, 15 Sep 2021 13:01:29 GMT

Justification for this deactivation request

This course used to be part of the core of the B.S. in Homeland Security at the DB campus. When the DB program was updated, this class was removed from the DB core. It will remain in the WW HLSD core. Neither program will be impacted by this course being deactivated on the DB campus.

Teach out Plan

None. Most DB students who required this class have graduated. Those who have not graduated take HS 220 - National Security Enterprise as a course substitute.

Plan for Student Notification

Any remaining students will be notified in advising, both through professional advising and faculty advising.

Proposer(s) Information

First Name	Last Name	Title	Email
Ann	Phillips		philla15@erau.edu

Primary Campus

Daytona Beach

Shared Campuses

Worldwide

Anticipated effective date for your proposal:

05/01/2022

DB College

Daytona College of Arts & Sciences

DB Department

Security Studies and International Affairs Dept

Course Level

Undergraduate

Course Prefix

HS

Course Number

280

Course Title

Professional Skills in Homeland Security

General Education Information

1. Lower level courses: First-year courses are foundation courses. They are wide-ranging, multidisciplinary overviews providing students with extensive opportunities to practice reading, research, and writing skills. Humanities, arts, social and natural science courses, particularly, should be broadly representative. Skills courses in mathematics, computer science/information technology, and physical and life sciences provide strong foundations for courses that follow them in the discipline.

2. Upper-level courses are broadly representative of a discipline or disciplines. Approved upper-level social science courses, for example, broadly study human experience, human society, and/or individual relationships in and to society. For example, history and geography courses address a broad swath of a period or region.

*Remember that course content and assignments should be include, but not limited to, research papers, projects, substantial creative projects, laboratory reports, mathematical analysis, etc.

Description

Course Description

Prepare students to seek and win internships. Personality evaluations, cover letter and resume preparation, interviewing skills. Ethics and professionalism in homeland security. Prerequisite is sophomore standing.

Criteria for General Education

Hours

Credit Hours

3

Components

Lecture

Prerequisites - Enforced

Sophomore standing;

Goals

Course Goals

This course introduces students to several skills that will assist their transition from a student to a professional and to begin a career in homeland security.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Measure and understand basic personality types.
2	Measure and understand a preferred conflict resolution style.
3	Discuss and relate the main characteristics of personality and conflict resolution style to career development.
4	Create a web page that can be used to advertise and market an individual.
5	Learn how to write a cover letter and resume and to tie them together.
6	Learn interviewing skills.

Learning Outcomes - University MCO

	Outcome
1	Measure and understand basic personality types.
2	Measure and understand a preferred conflict resolution style.

3	Discuss and relate the main characteristics of personality and conflict resolution style to career development.
4	Create a web page that can be used to advertise and market an individual.
5	Learn how to write a cover letter and resume and to tie them together.
6	Learn interviewing skills.

Reviewer Comments

Taylor Mitchell (mitcht15) (Wed, 15 Sep 2021 03:01:16 GMT): Rollback: Course Description: N/A Goals: N/A Student Learning Outcomes: Ensure SLO #1, 2, 3, and 5 only have one action verb; Avoid using understand

Key: 2381

History

1. Mar 4, 2022 by Ann Phillips (philla15)

HSI 290: INTRODUCTION TO ENVIRONMENTAL SECURITY

Viewing: HSI 290 : Introduction to Environmental Security

Formerly known as: HS 290

Last approved: Wed, 16 Mar 2022 08:00:39 GMT

Last edit: Tue, 15 Feb 2022 21:33:47 GMT

Proposer(s) Information

First Name	Last Name	Title	Email
Ann	Phillips	Program Coordinator for Homeland Security	philla15@erau.edu

Primary Campus
Daytona Beach

Anticipated effective date for your proposal:
05/01/2022

DB College
Daytona College of Arts & Sciences

DB Department
Security Studies and International Affairs Dept

Course Level
Undergraduate

Course Prefix
HSI

Course Number
290

Course Title
Introduction to Environmental Security

Is this a Gen Ed course?
No

Detailed Description of Proposed Change
Change the title of the course to Introduction to Environmental and Human Security to better reflect the content of the course
Change the prefix to HSI
Update course description, goals, and learning outcomes to comply with new AP05 guidance and to reflect the focus on humans and sustainability

Description

Course Description
Environmental issues related to socio-political instability around the world. Development and execution of U.S. domestic and foreign policy, and ultimately U.S. national security. Emerging threats to nations from environmental health issues, infrastructure vulnerabilities, and natural resource shortages caused by rapid industrialization, population growth, and urbanization in less developed countries. Transnational threats from ozone depletion, deforestation, and climate change.

Hours

Credit Hours
3

Components
Lecture

Lecture Hours per week

3

Prerequisites - Enforced

HSI 110;

Teaching Disciplines

Civics / Economics / Environmental Science / Environmental Policy / Geography / Government / Health Services Research / History / Homeland Security / Intelligence Studies / International Affairs / International Relations/ Law / Military Technologies / National Security / Political Science / Politics / Population Health / Public Health / Social Science / Sociology / Strategic Studies

Related Disciplines

Emergency Management / Foreign Affairs / Environmental Engineering / Energy Policy and Climate / Human Security / Global Conflict Studies

Goals

Course Goals

Develop an understanding of how diverse disciplines such as environmental health, environmental science, meteorology, climatology, international relations, homeland security, human security, and national security studies can come together to address some very complex issues that have potentially global impacts.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Explain the destabilizing influences of environmental changes, such as reducing access to fresh water, impairing food production, contributing to or causing health catastrophes, causing land losses, flooding, and population displacement.
2	Identify the growing role that the natural environment plays in contributing to or causing destabilization within a country or within a region, and how this destabilization can lead to security concerns for the U.S. and its allies.
3	Debate the security implications of environmental changes, such as greater potential for failed states and growth of terrorism, mass migrations, and potential conflicts over limited resources within or between countries.
4	Investigate how Sustainable Development can serve as a framework for potential solutions to the challenges of human insecurity.
5	Discuss how human security relates to socio-political insecurity specifically in the areas of economics, health, environment, politics, food, personal, and community safety.

Learning Outcomes - University MCO

	Outcome
1	Explain the destabilizing influences of environmental changes, such as reducing access to fresh water, impairing food production, contributing to or causing health catastrophes, causing land losses, flooding, and population displacement.
2	Identify the growing role that the natural environment plays in contributing to or causing destabilization within a country or within a region, and how this destabilization can lead to security concerns for the U.S. and its allies.
3	Debate the security implications of environmental changes, such as greater potential for failed states and growth of terrorism, mass migrations, and potential conflicts over limited resources within or between countries.
4	Investigate how Sustainable Development can serve as a framework for potential solutions to the challenges of human insecurity.
5	Discuss how human security relates to socio-political insecurity specifically in the areas of economics, health, environment, politics, food, personal, and community safety.

Proposal Details

Describe the need and rationale for the modifications proposed.

Updates prefix to reflect the new degree and program title.

Brings current the course description, goals, and learning outcomes to comply with new AP05 guidance. The added learning objectives more specifically address/measure the human security aspects of the course.

What programs accept this course as an elective?

Affected Programs
DBSHSI - B.S. in Homeland Security and Intelligence

Cost

Provide a detailed cost estimate for the proposed course.

No costs will be incurred with this proposal

Impact

Specify which programs will be affected by this proposed change.

Affected Programs
DBSHSI - B.S. in Homeland Security and Intelligence

Specify effect on facilities and equipment.

There will be no impact on facilities

Additional Information

Key: 2383

History

1. Mar 16, 2022 by Ann Phillips (philla15)

HSI 320: HOMELAND SECURITY AND INTELLIGENCE LAW AND POLICY

Viewing: HSI 320 : Homeland Security and Intelligence Law and Policy

Formerly known as: HS 320

Last approved: Sat, 19 Feb 2022 09:00:44 GMT

Last edit: Fri, 18 Feb 2022 20:39:56 GMT

Proposer(s) Information

First Name	Last Name	Title	Email
Ann	Phillips	Program Coordinator for Homeland Security	phila15@erau.edu

Primary Campus
Daytona Beach

Anticipated effective date for your proposal:
05/01/2022

DB College
Daytona College of Arts & Sciences

DB Department
Security Studies and International Affairs Dept

Course Level
Undergraduate

Course Prefix
HSI

Course Number
320

Course Title
Homeland Security and Intelligence Law and Policy

Is this a Gen Ed course?
No

Detailed Description of Proposed Change
Change prefix to HSI
Update title
Update course description, goals, and learning outcomes to comply with new AP05 guidance

Description

Course Description
Key legal, policy, and ethical issues in the context of Homeland Security and Intelligence policy and practice. Examine legal concepts regarding constitutional rights of individuals, legal process, access to courts, the law of war, and national security principles as they relate to homeland security legislation and policy initiatives. Legal principles of due process, habeas corpus, search and seizure, compulsory process, and international agreements are explored. Elements of national security law, including intelligence collection and sharing, the Patriot Act, and military-civilian relations. Analyze recent Supreme Court decisions relating to applicable concepts and legal principles.

Hours

Credit Hours
3

Components
Lecture

Lecture Hours per week
3

Prerequisites - Enforced
HSI 215;

Teaching Disciplines
Civics / Government / History / Homeland Security / Intelligence Studies / Law / National Security / Political Science / Politics / Public Policy / Security / Security Management / Social Science / Strategic Studies / Terrorism Studies

Related Disciplines
International Affairs / International Relations / Public Policy / Public Policy Administration / Law Enforcement

Goals

Course Goals
This course introduces students to the goals and challenges of homeland security and intelligence law, policy, and legislation in the U.S. today.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Discuss critical definitions of law as they apply to Homeland Security and Intelligence.
2	Analyze U.S. regulatory authority (Patriot Act, HSPD's, etc.) regarding homeland security and key legislative efforts on behalf of Homeland Security, Intelligence, and defense.
3	Break down the interrelationships between law enforcement, intelligence, and security, and the respective roles of local, state, and federal law enforcement agencies.
4	Compare core components of constitutional and international law principles and their relationship to Homeland Security and Intelligence efforts.
5	Discuss challenges to Homeland Security and Intelligence legislation and policy posed by legal issues and evolving notions of national security strategy.

Learning Outcomes - University MCO

	Outcome
1	Discuss critical definitions of law as they apply to Homeland Security and Intelligence.
2	Analyze U.S. regulatory authority (Patriot Act, HSPD's, etc.) regarding homeland security and key legislative efforts on behalf of Homeland Security, Intelligence, and defense.
3	Break down the interrelationships between law enforcement, intelligence, and security, and the respective roles of local, state and federal law enforcement agencies.
4	Compare core components of constitutional and international law principles and their relationship to Homeland Security and Intelligence efforts.
5	Discuss challenges to Homeland Security and Intelligence legislation and policy posed by legal issues and evolving notions of national security strategy.

Proposal Details

Describe the need and rationale for the modifications proposed.
Updates prefix to reflect the new degree and program title
Brings current the course title, description, goals, and learning outcomes to comply with new AP05 guidance

What programs accept this course as an elective?

Affected Programs
DBSCS - B.S. in Computer Science
DMHOMESEC - Homeland Security
DMUASPS - Uncrewed Aircraft Systems (UAS) Public Safety
DMAVILAW - Aviation Law

Cost

Provide a detailed cost estimate for the proposed course.

No costs will be incurred with this proposal

Impact

Specify which programs will be affected by this proposed change.

Affected Programs
DBSHSI - B.S. in Homeland Security and Intelligence
DMAVILAW - Aviation Law
DMHOMESEC - Homeland Security
DMUASPS - Uncrewed Aircraft Systems (UAS) Public Safety

Specify effect on facilities and equipment.

There will be no impact on facilities

Additional Information

Reviewer Comments

Taylor Mitchell (mitcht15) (Thu, 03 Feb 2022 18:25:31 GMT): Since HS 110 is a prereq to HS 215, "Prereq - Enforced" only needs to be HS 215

Key: 2388

History

1. Feb 19, 2022 by Ann Phillips (philla15)

HSI 323: GOVERNMENT OF THE U.S.

Viewing: HSI 323 : Government of the U.S.

Formerly known as: HS 323

Last approved: Fri, 18 Mar 2022 08:01:25 GMT

Last edit: Thu, 17 Feb 2022 20:47:37 GMT

Proposer(s) Information

First Name	Last Name	Title	Email
Ann	Phillips	Program Coordinator for Homeland Security	philla15@erau.edu

Primary Campus

Daytona Beach

Shared Campuses

Prescott
Worldwide

Shared Campus Comments

The only change is to the prefix (from HS to HSI) so I did not reach out to the other campuses. The SLOs, course description, and course goals were updated in coordination with the other campuses last year when the prefix changed from SS to HS.

Anticipated effective date for your proposal:

05/01/2022

DB College

Daytona College of Arts & Sciences

DB Department

Security Studies and International Affairs Dept

Course Level

Undergraduate

Course Prefix

HSI

Course Number

323

Course Title

Government of the U.S.

Is this a Gen Ed course?

Yes

Detailed Description of Proposed Change

Change the prefix from HS to HSI in coordination with all the other courses which are part of the HS/HSI degree program.
The course status as a gen ed course will remain as is.

Description

Course Description

Introduction to basic issues of democracy in the U.S.; constitutional principles; the executive, legislative and judicial branches of government.

Hours

Credit Hours

3

Components
Lecture

Lecture Hours per week
3

Prerequisites - Enforced
SS Lower Level General Education Equivalent; any lower level SS or GCS course

Teaching Disciplines
Political Science / Politics / Government / History

Related Disciplines
National Security / Law / International Relations / Civics

Goals

Course Goals
This course is designed to develop an understanding of the political world in the United States. It introduces the nature of constitutional government at the national level, contributing to a greater understanding and political awareness among an informed citizenry. Students are introduced to rules, institutions and concepts in order to demonstrate the allocation of power and resources in political conflict, supporting an understanding that the U.S. political process inevitably involves its citizens, regardless of their involvement in politics. A research paper is required.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - DB

	Outcome
1	Examine political, economic, educational terms.
2	Evaluate the American System of Government with other systems.
3	Judge the effectiveness of public opinion and the role of mass media by describing specific events of historical significance with today's headline news.
4	Identify current governmental decisions affecting citizens.
5	Analyze past, contemporary, or current issues or problems impacting the function of the U.S. government in a formal research paper.

Learning Outcomes - University MCO

	Outcome
1	Examine political, economic, educational terms.
2	Evaluate the American System of Government with other systems.
3	Judge the effectiveness of public opinion and the role of mass media by describing specific events of historical significance with today's headline news.
4	Identify current governmental decisions affecting citizens.
5	Analyze past, contemporary, or current issues or problems impacting the function of the U.S. government in a formal research paper.

Proposal Details

Describe the need and rationale for the modifications proposed.
We are proposing to change the prefix of HS 323 - Government of the U.S. to HSI 323 Government of the U.S. This course was recently been revived on the Daytona Beach campus and has is being added to the HSI core. The course contains content vital to the Homeland Security and Intelligence major and its learning outcomes reflect the HSI discipline. This change better keeps the prefix consistent within the degree program while retaining its status as a course that satisfies General Education requirements.

This course supports the HSI goals and should be designated similarly to existing HSI-named courses.

What programs accept this course as an elective?

Affected Programs
DBSGCS - B.S. in Global Conflict Studies
DBSIS - B.S. in Interdisciplinary Studies
DMINTHIST - International History
DMTERRSTUD - Terrorism Studies
DMGCS - Global Conflict Studies

Will/Does this course serve as a prerequisite or corequisite for any other courses?
No

Cost

Provide a detailed cost estimate for the proposed course.
There is no cost associated with this course.

Impact

Specify which programs will be affected by this proposed change.

Affected Programs
DBSHSI - B.S. in Homeland Security and Intelligence
DBSGCS - B.S. in Global Conflict Studies
DMINTHIST - International History
DMGCS - Global Conflict Studies
DMTERRSTUD - Terrorism Studies
DBSIS - B.S. in Interdisciplinary Studies

Specify effect on facilities and equipment.
No additional facilities, equipment, or faculty will be required to offer this course now or in the near future.

Additional Information

Reviewer Comments
Matthew Sharp (sharpm2) (Thu, 16 Dec 2021 18:24:05 GMT): Change to HSI in the dropdown.

Key: 4599

History

1. Jul 6, 2021 by Kimberly Staley (stale1ed)
2. Nov 9, 2021 by Janel Wilson (wilsoj45)
3. Mar 18, 2022 by Ann Phillips (philla15)

COURSE PROPOSAL

Viewing: MHSR 515 : International Law and U.S. Security Policy

Primary Campus
Worldwide

WW College
Worldwide College of Arts & Sciences

WW Department
Security and Emergency Services

Course Level
Masters

Course Prefix
MHSR

Course Number
515

Course Title
International Law and U.S. Security Policy

Description

Course Description
The course examines the role of international law, U.S. foreign policy, and international institutions in responding to terrorism, crime, complex emergencies, disasters and crises. It analyzes the challenges and difficulties in achieving unified response and the administrative and legal barriers that must be overcome. The course discusses how U.S. laws and policies intersect with international norms and regimes in a US security context, including existing multinational treaties such as UNCLOS and the Antarctic Treaty System, International Cybercrime Treaty, the Biological Weapons Convention or the Chemical Weapons Convention, and international humanitarian law. Particular attention is paid to privacy laws. The conflicts that are caused by disparate laws and policies will also be explored, as well as challenges to solutions.

Hours
Credit Hours
3

Components
Lecture

Teaching Disciplines
Homeland Security
Criminal Justice
Criminology
Public Policy Administration
Emergency Management
Law
Political Science
Terrorism Studies
Intelligence Studies
Transportation Logistics
Security Management
Security Services
Public Health
Sociology

Related Disciplines
Population Health
Cyber Security
Foreign Services
Forensics
Health Services Research
Military Technologies
Public Policy
Safety Management
Security Services
Computer Technology
International Relations
History
Geography
International Affairs
Politics

Goals

Course Goals
This course surveys the principle domestic legal constraints the U.S. government must operate within when pursuing U.S. security interests around the globe and in cyberspace. Students will be exposed to the main legal constructs of domestic and international laws which affect the United Statesrsquo; ability to formulate and execute its security policies regarding a wide range of national interests in both the "real" world and the virtual world.

This is a required course for the M.S. in Cybersecurity Management & Policy and M.S. in Human Security & Resilience programs. It must be taken after MCMP/MHSR 501 and should be taken after at least one other 500-level course in the student's program.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - University MCO

	Outcome
1	Identify and evaluate legal aspects of U.S. security issues or challenges through the use existing national and international laws, treaties, and cases.
2	Identify the growing role that global trends and activities have upon U.S. security concerns.
3	Analyze the policy objectives of the U.S. regarding national, human, and cybersecurity, and compare and contrast those objectives with current laws and policies.
4	Confront unfamiliar real-world problems involving security, terrorism, crime, complex emergencies, disasters, crises, and cyberspace in light of existing laws and policies, both nationally and internationally.
5	Demonstrate the ability to synthesize, analyze, and evaluate U.S. security issues, challenges, and their associated legal aspects.

Learning Outcomes - WW

	Outcome
1	Identify and evaluate legal aspects of U.S. security issues or challenges through the use existing national and international laws, treaties, and cases.
2	Identify the growing role that global trends and activities have upon U.S. security concerns.
3	Analyze the policy objectives of the U.S. regarding national, human, and cybersecurity, and compare and contrast those objectives with current laws and policies.
4	Confront unfamiliar real-world problems involving security, terrorism, crime, complex emergencies, disasters, crises, and cyberspace in light of existing laws and policies, both nationally and internationally.

5	Demonstrate the ability to synthesize, analyze, and evaluate U.S. security issues, challenges, and their associated legal aspects.

Proposal Details

Need or Rationale

Cost

Impact

Additional Information

Key: 3171

MCMP 516: AVIATION POLICY AND LAW IN CYBERSPACE

Course Deactivation Proposal
Viewing: MCMP 516 : Aviation Policy and Law in Cyberspace
Last approved: Tue, 15 Feb 2022 09:03:52 GMT
Last edit: Wed, 19 Jan 2022 14:58:27 GMT

Justification for this deactivation request

MCMP 516 will updated to MACY 526 that will be one of the 10 courses for the Master of Aviation Cybersecurity (WMAC) program.

Teach out Plan

MACY 526 will be a direct substitute (over 75% overlap of LOs) for MCMP 516 for students in the MSCMP program.

Plan for Student Notification

We will brief change to Academic Advising so they can inform students.

Proposer(s) Information

First Name	Last Name	Title	Email
David	Harvie		harvied@erau.edu

Primary Campus

Worldwide

Anticipated effective date for your proposal:

07/01/2022

WW College

Worldwide College of Aviation

WW Department

Department of Graduate Studies

Course Level

Masters

Course Prefix

MCMP

Course Number

516

Course Title

Aviation Policy and Law in Cyberspace

General Education Information

1. Lower level courses: First-year courses are foundation courses. They are wide-ranging, multidisciplinary overviews providing students with extensive opportunities to practice reading, research, and writing skills. Humanities, arts, social and natural science courses, particularly, should be broadly representative. Skills courses in mathematics, computer science/information technology, and physical and life sciences provide strong foundations for courses that follow them in the discipline.

2. Upper-level courses are broadly representative of a discipline or disciplines. Approved upper-level social science courses, for example, broadly study human experience, human society, and/or individual relationships in and to society. For example, history and geography courses address a broad swath of a period or region.

*Remember that course content and assignments should be include, but not limited to, research papers, projects, substantial creative projects, laboratory reports, mathematical analysis, etc.

Description

Course Description

This course addresses emerging policies and laws that affect cyberspace, particularly related to information security and cybercrime in the aviation and aerospace industry. The clash between real space and cyberspace is examined, as well as international laws and policies related to aviation, aerospace, and aeronautics.

Criteria for General Education

Hours

Credit Hours

3

Components

Lecture

Teaching Disciplines

Homeland Security
Computer Technology
Criminal Justice
Criminology
Cyber Security
Emergency Management
Law
Political Science
Public Policy Administration
Terrorism Studies
Intelligence Studies
Transportation Logistics
Security Management
Security Services

Related Disciplines

Population Health
Foreign Services
Forensics
Health Services Research
Military Technologies
Public Policy
Safety Management
Security Services
International Relations
History
Geography
International Affairs
Politics

Goals

Course Goals

The goal of this course is to make students aware of the role of law and policy in cyberspace, particularly as it affects aviation, aerospace, and aeronautics. Although it is common to explain activities and issues in cyberspace by way of comparison or analogy with the physical world, it is imperative that students actually see cyberspace as a world unto itself, in an environment that is more than a 'virtual copy of the real world'. To that end, the course explores crime, information security, international law, cyber warfare, and other aspects of human life that impact the aviation industry in a virtual world.

Outcomes

Instructions: Use the Green Plus (+) sign to add each learning outcome on a separate row, with a period at the end of each sentence.

Learning Outcomes - University MCO

	Outcome
1	Compare and contrast physical space and cyberspace in terms of policy, law, society, rights, and security, with particular emphasis on the aviation industry.
2	Articulate the role of national and international laws in cyberspace, as well as cyber laws affecting aviation.
3	Examine the rights of users in cyberspace, including freedom of expression, privacy, and anonymity.
4	Analyze the cybersecurity policies of the U.S. and international bodies, the protection of critical infrastructures, and the cyber safety of aviation.
5	Produce a set of recommendations to better secure aviation industrial sector from threats -- and opportunities – in cyberspace.

Learning Outcomes - WW

	Outcome
1	Compare and contrast physical space and cyberspace in terms of policy, law, society, rights, and security, with particular emphasis on the aviation industry.
2	Articulate the role of national and international laws in cyberspace, as well as cyber laws affecting aviation.
3	Examine the rights of users in cyberspace, including freedom of expression, privacy, and anonymity.
4	Analyze the cybersecurity policies of the U.S. and international bodies, the protection of critical infrastructures, and the cyber safety of aviation.
5	Produce a set of recommendations to better secure aviation industrial sector from threats – and opportunities – in cyberspace.

Reviewer Comments

Jonathan Campbell (campb8c1) (Wed, 19 Jan 2022 23:02:11 GMT): no issues or concerns at this time ... best

Debra Bourdeau (taylo13f) (Thu, 20 Jan 2022 15:08:01 GMT): Senate Graduate Curriculum Committee concurs.

Linda Rowell (rowelll) (Thu, 03 Feb 2022 18:52:55 GMT): 2 week review complete. Proposal advanced.

Linda Rowell (rowelll) (Mon, 14 Feb 2022 20:08:54 GMT): Curriculum approved effective 7-1-2022.

Key: 2826

History

1. Apr 12, 2021 by Joan Jiminez (jiminezj)
2. Feb 15, 2022 by David Harvie (harvied)

CERTIFICATE

I have read the foregoing questions carefully and have answered them truthfully, fully and completely. I hereby waive notice by and authorize The Florida Bar or any of its committees, educational and other institutions, the Judicial Qualifications Commission, the Florida Board of Bar Examiners or any judicial or professional disciplinary or supervisory body or commission, any references furnished by me, employers, business and professional associates, all governmental agencies and instrumentalities and all consumer and credit reporting agencies to release to the respective Judicial Nominating Commission and Office of the Governor any information, files, records or credit reports requested by the commission in connection with any consideration of me as possible nominee for appointment to judicial office. Information relating to any Florida Bar disciplinary proceedings is to be made available in accordance with Rule 3-7.1(l), Rules Regulating The Florida Bar. I recognize and agree that, pursuant to the Florida Constitution and the Uniform Rules of this commission, the contents of this questionnaire and other information received from or concerning me, and all interviews and proceedings of the commission, except for deliberations by the commission, shall be open to the public.

Further, I stipulate I have read and understand the requirements of the Florida Code of Judicial Conduct.

Dated this 8th day of January 2024.

Ann Phillips
Printed Name

Ann Phillips
Signature

(Pursuant to Section 119.071(4)(d)(1), F.S.), . . . *The home addresses and telephone numbers of justices of the Supreme Court, district court of appeal judges, circuit court judges, and county court judges; the home addresses, telephone numbers, and places of employment of the spouses and children of justices and judges; and the names and locations of schools and day care facilities attended by the children of justices and judges are exempt from the provisions of subsection (1), dealing with public records.*

FINANCIAL HISTORY

1. State the amount of gross income you have earned, or losses you have incurred (before deducting expenses and taxes) from the practice of law for the preceding three-year period. This income figure should be stated on a year to year basis and include year to date information, and salary, if the nature of your employment is in a legal field.

Current Year-To-Date: 2024 to date/ $0
Last Three Years: 2023/ $0
2022/ $8,000
2021/ $0

2. State the amount of net income you have earned, or losses you have incurred (after deducting expenses but not taxes) from the practice of law for the preceding three-year period. This income figure should be stated on a year to year basis and include year to date information, and salary, if the nature of your employment is in a legal field.

Current Year-To-Date: 2024 to date/ $0
Last Three Years: 2023/ $ 0
2022/ $6,776
2021/ $0

3. State the gross amount of income or losses incurred (before deducting expenses or taxes) you have earned in the preceding three years on a year by year basis from all sources other than the practice of law, and generally describe the source of such income or losses.

Current Year-To-Date: 2024/ $0 — ERAU/employer
Last Three Years: 2023/ $98,064 - ERAU/employer
2022/ $98,455 – ERAU/employer
2021/ $79,537 – ERAU/employer

4. State the amount you have earned in the preceding three years on a year by year basis from all sources other than the practice of law, and generally describe the source of such income or losses.

Current Year-To-Date: 2024/ $0 — ERAU/employer
Last Three Years: 2023/ $98,064 — ERAU/employer
2022/ $98,455 – ERAU/employer
2021/ $79,537 – ERAU/employer

5. State the amount of net income you have earned or losses incurred (after deducting expenses) from all sources other than the practice of law for the preceding three-year period on a year by year basis, and generally describe the sources of such income or losses.

Current Year-To-Date: 2024/ $ 0
Last Three Years: 2023/ $52,257— ERAU/employer
2022/ $66,808 – ERAU/employer
2021/ $75,493 – ERAU/employer

FORM 6
FULL AND PUBLIC

DISCLOSURE OF
FINANCIAL INTEREST

PART A – NET WORTH

Please enter the value of your net worth as of December 31 or a more current date. [Note: Net worth is not calculated by subtracting your *reported* liabilities from your *reported* assets, so please see the instructions on page 3.]

My net worth as of December 31, 2023, was $ 1,641,534.

PART B - ASSETS

HOUSEHOLD GOODS AND PERSONAL EFFECTS:

Household goods and personal effects may be reported in a lump sum if their aggregate value exceeds $1,000. This category includes any of the following, if not held for investment purposes; jewelry; collections of stamps, guns, and numismatic items; art objects; household equipment and furnishings; clothing; other household items; and vehicles for personal use.

The aggregate value of my household goods and personal effects (described above) is $95,000

ASSETS INDIVIDUALLY VALUED AT OVER $1,000:

DESCRIPTION OF ASSET (specific description is required – see instructions p. 3)	VALUE OF ASSET
Real Property – [redacted], Ormond Beach, FL (tenancy by the entirety)	$489,000
Wells Fargo (joint checking with spouse)	$36,288
Wells Fargo (joint savings with spouse)	$262,386
Bank of America stock (joint with spouse)	$49,995
Verizon stock (joint with spouse)	$5,888
AT&T stock (joint with spouse)	$3,267

PART C - LIABILITIES

LIABILITIES IN EXCESS OF $1,000 (See instructions on page 4): NAME AND ADDRESS OF CREDITOR	AMOUNT OF LIABILITY
Real Property private loan - [redacted] (joint with spouse)	$250,000

JOINT AND SEVERAL LIABILITIES NOT REPORTED ABOVE: NAME AND ADDRESS OF CREDITOR	AMOUNT OF LIABILITY

PART D - INCOME

You may ***EITHER*** (1) file a complete copy of your latest federal income tax return, *including all W2's, schedules, and attachments,* ***OR*** (2) file a sworn statement identifying each separate source and amount of income which exceeds $1,000 including secondary sources of income, by completing the remainder of Part D, below.

☐ I elect to file a copy of my latest federal income tax return and all W2's, schedules, and attachments.
(if you check this box and attach a copy of your latest tax return, you need *not* complete the remainder of Part D.]

PRIMARY SOURCE OF INCOME (See instructions on page 5):

NAME OF SOURCE OF INCOME EXCEEDING $1,000	ADDRESS OF SOURCE OF INCOME	AMOUNT
Embry-Riddle Aeronautical University	1 Aerospace Blvd., Daytona Beach, FL 32114	$98,067
Bank of America dividends/capital gains (joint w/ spouse)	100 N. Tryon St., Charlotte, NC 28255	$1,222

SECONDARY SOURCES OF INCOME [Major customers, clients, etc., of businesses owned by reporting person—see instructions on page 6]

NAME OF BUSINESS ENTITY	NAME OF MAJOR SOURCES OF BUSINESS' INCOME	ADDRESS OF SOURCE	PRINCIPAL BUSINESS ACTIVITY OF SOURCE

PART E – INTERESTS IN SPECIFIC BUSINESS [Instructions on page 7]

	BUSINESS ENTITY #1	BUSINESS ENTITY #2	BUSINESS ENTITY #3
NAME OF BUSINESS ENTTITY			
ADDRESS OF BUSINESS ENTITY			
PRINCIPAL BUSINESS ACTIVITY			
POSITION HELD WITH ENTITY			
I OWN MORE THAN A 5% INTEREST IN THE BUSINESS			
NATURE OF MY OWNERSHIP INTEREST			

IF ANY OF PARTS A THROUGH E ARE CONTINUED ON A SEPARATE SHEET, PLEASE CHECK HERE ☐

OATH

I, the person whose name appears at the beginning of this form, do depose on oath or affirmation and say that the information disclosed on this form and any attachments hereto is true, accurate, and complete.

Ann Phillips

SIGNATURE

STATE OF FLORIDA

COUNTY OF Volusia

Sworn to (or affirmed) and subscribed before me this 7th day of Jan, 2024 by Ann M. Phillips

MaryEllen P. Osterndorf

(Signature of Notary Public—State of Florida)

MaryEllen P. Osterndorf

(Print, Type, or Stamp Commissioned Name of Notary Public)

Personally Known X *OR* Produced Identification _____

Type of Identification Produced _____

NOTARY PUBLIC STATE OF FLORIDA
MARYELLEN P. OSTERNDORF
Commission # GG 979202
Expires June 24, 2024
Bonded Thru Budget Notary Services

PART B – ASSETS (cont'd)

TIAA Retirement Account	**$868,055**
Investment Property- [redacted]	**$299,000**

JUDICIAL APPLICATION DATA RECORD

The judicial application shall include a separate page asking applicants to identify their race, ethnicity and gender. Completion of this page shall be optional, and the page shall include an explanation that the information is requested for data collection purposes in order to assess and promote diversity in the judiciary. The chair of the Commission shall forward all such completed pages, along with the names of the nominees to the JNC Coordinator in the Governor's Office (pursuant to JNC Uniform Rule of Procedure).

(Please Type or Print)

Date: January 8, 2024

JNC Submitting To: Seventh Judicial Circuit

Name (please print): Ann M. Phillips

Current Occupation: Associate Professor

Telephone Number: [redacted] Attorney No.: 978698

Gender (check one): ☐ Male ☒ Female

Ethnic Origin (check one):
- ☒ White, non-Hispanic
- ☐ Hispanic
- ☐ Black
- ☐ American Indian/Alaskan Native
- ☐ Asian/Pacific Islander

County of Residence: Volusia

FLORIDA DEPARTMENT OF LAW ENFORCEMENT

DISCLOSURE PURSUANT TO THE
FAIR CREDIT REPORTING ACT (FCRA)

The Florida Department of Law Enforcement (FDLE) may obtain one or more consumer reports, including but not limited to credit reports, about you, for employment purposes as defined by the Fair Credit Reporting Act, including for determinations related to initial employment, reassignment, promotion, or other employment-related actions.

CONSUMER'S AUTHORIZATION FOR
FDLE TO OBTAIN CONSUMER REPORT(S)

I have read and understand the above Disclosure. I authorize the Florida Department of Law Enforcement (FDLE) to obtain one or more consumer reports on me, for employment purposes, as described in the above Disclosure.

Ann Phillips

Printed Name of Applicant

Ann Phillips

Signature of Applicant

Date: January 8, 2024