Explore Topics: Rights, Privacy, Security

Kevin Barnes

General Instructions

1. For each page, synthesize the reading and research by writing in complete sentences in essay format.
   a. Use the green instructions in the notes below each page to focus your research and writing.
   b. Write about each question, prompt, or process provided in those notes.
   c. Write a full page of text with lots of detail (more than 250 words).
      i. Don’t generalize so much that your writing is devoid of detail.
      ii. Don’t repeat yourself.
   d. Cite each source by adding a hyperlink in the Title of the Article or law.
   e. Do not change the template:
      i. Text must be 14 point Lato left-justified type.
      ii. Refrain from adding extra margins or double spacing.
      iii. Do not bullet the paragraphs. Write in essay format only.
   f. Add additional pages if you need more room.

2. Add all sources to the Bibliography page.
   a. Include author, year, title, publisher, and URL.
   b. Number or bullet them using the list button.

When in doubt, write to the instructor for clarification using the Canvas Inbox.
The Fourth Amendment generally protects Americans from unreasonable searches and seizures. In “Know Your Rights” (2014), Fakhoury and Kayyali explore the specific ways courts have interpreted this right, and the legal framework that now exists regarding law enforcement searches in the United States. The police generally need a warrant to enter and search your home. If the police produce a warrant and demand to search an individual’s home, it will be limited in scope in a variety of ways. It is important to ask to see the warrant and read it to determine what place, people, and items can be searched and when the search must be executed. The subject of the search warrant is not obligated to help law enforcement. This lack of obligation extends to circumstances in which a person’s electronic devices are seized in a police search; one is not usually required to hand over codes, encryption keys, or passwords to police. Police are allowed to perform searches of homes in two circumstances without a warrant. The first is when they are given permission to do the search by someone who has, or who police reasonably believe has, authority to allow them into the home. There is no benefit to giving police permission to search one’s home, and people are encouraged to require law enforcement to go through the warrant process. The second situation in which police may perform a warrantless search is when they have probable cause to believe that there is an imminent threat of evidence inside the home being destroyed. Whether the police have a warrant or not, it is important for Americans to recognize that there is little benefit to assisting police with their investigation, including through answering questions. As James Duane explains in “Don’t Talk to the Police” (2012), there is almost never an upside to
assisting a police investigation. Because of peculiarities in the American criminal justice system there is almost never a situation in which the assistance of a suspected individual will help that person in court. Conversely, there are strong rules preventing the prosecution from using the fact that the accused individual asserted their rights as evidence against them. This creates an incentive structure in which citizens have no reason to cooperate with law enforcement investigations.
The U.S. Department of Justice (DOJ) report “The USA PATRIOT Act: Preserving Life and Liberty” (2020) describes many of the intended benefits of the Patriot Act, passed in the wake of the September 11th terrorist attacks in 2001. The Patriot Act provides a legal path for a variety of evidence gathering tools including general surveillance, secret warrant processes, business record warrants, and changes the warrant application process to streamline the warrant process for investigators. The Patriot Act also provides a legal framework which law enforcement can use to more effectively coordinate their investigations, particularly with regard to terrorism. Finally, the Patriot Act provides for new or enhanced criminal penalties on a number of existing crimes which the DOJ says are related to terrorist activities.

The Patriot Act has also faced a large amount of criticism for both the content of the law and its real-world application. In “Myths and Realities About the Patriot Act” (2020), the American Civil Liberties Union (ACLU) attacks many of the federal government’s claims about the Patriot Act and its usage. The ACLU points out that the powers granted to law enforcement by the Patriot Act have been abused for purposes beyond those laid out by the DOJ in a number of cases which have come under public scrutiny, and an unknown number of cases which remain secret. They also dispute the government’s characterization of the legal changes within the Patriot Act as a simple update; many of the powers granted by the Patriot Act overturn existing standards such as the “seven day rule” for delayed notice warrants and allowing domestic investigations of terrorism suspects to use tools historically reserved for
international terrorism cases. The ACLU also alleges that powers created in the Patriot Act don’t exist to create a communication conduit between intelligence services and law enforcement because the tools for that kind of cooperation already existed through the sharing of FISA warrant information. Instead, they say, the Patriot Act serves primarily to make it easier for government agents to operate around the Fourth Amendment rights of Americans.
In “What are deepfakes – and how can you spot them?” (2020) Ian Sample lays out the technology around deepfakes and their implications for society. Deepfakes are a form of manipulated image or video created using AI learning. To create them, a large amount of visual examples of a person are fed into an AI algorithm, which learns the structure and appearance of that person’s face. Another algorithm is then used to map those facial features onto an existing image or series of images (such as frames of a video). The result is a video which progresses exactly as the original video did, but with a new person’s face seamlessly inserted over the original. Given enough AI learning time and information, and finishing touches by a human graphic artist, the final product looks completely real. To further increase the effectiveness of a deepfake, a “voice skin” can be created using a similar AI process to make the voice of the speaker in a deepfake match the simulated face. Though they have only existed since about 2017, the implication of the existence of deepfakes is beginning to set in. According to Rob Toews in “Deepfakes Are Going To Wreak Havoc On Society. We Are Not Prepared” (2020), the potential nefarious uses for deepfakes are incredibly broad. They could be used to damage the reputations of anyone with enough public images to allow the AI to work. They could be used to fabricate disasters, damage public trust in institutions or people, or even influence elections. To make matters worse, the infrastructure required to make use of deepfake technology is available to nearly anyone with a reasonably powerful computer. Equally chilling is the converse concern; the existence of deepfakes in the wild casts doubt on the veracity of any real video that doesn’t suit the priors of the viewer. It’s another technology which serves to raise the walls on the information silos in which we live.
In “Rebooting Computer Crime Law Part 1: No Prison Time For Violating Terms of Service” (2013) by Marcia Hofmann and Rainey Reitman, “Rebooting Computer Crime Law Part 2: Protect Tinkerers, Security Researchers, Innovators, and Privacy Seekers” (2013) by Cindy Cohn and Marcia Hofmann, and “Rebooting Computer Crime Part 3: The Punishment Should Fit the Crime” by Cindy Cohn, Hanni Fakhoury, and Marcia Hofmann, the Electronic Frontier Foundation (EFF) lays out their suggested changes to the Computer Fraud and Abuse Act (CFAA), a law which has been updated many times since it was originally passed in 1986. The EFF claims that the largest problem with the CFAA is that its ambiguous language leaves open the possibility of arguing that it actually criminalizes violations of terms of service on computer software and websites (Hofmann & Reitman 2013). This line of thinking would criminalize relatively innocuous behavior like lying about one’s age on a website or being rude on many web forums. The EFF says that minor infractions of this nature shouldn’t be met with large fines, jail time, or other criminal penalties. Additionally, the CFAA treats any computer user who attempts to avoid identity tracking as criminals (Cohn & Hofmann 2013). There are many harmless reasons to avoid this sort of tracking, including personal privacy, software creation, security research, and troubleshooting technological problems. The EFF proposes that any harmful activity which is facilitated by identity obfuscation should be criminalized, not the obfuscation itself. Finally, the EFF recommendation attempts to bring penalties under the CFAA in line with the conduct they are punishing (Cohn et al. 2013). The CFAA has a sliding scale for sentencing which punished a defendant more harshly if
they have committed crimes previously under the CFAA. While this seems reasonable as a deterrent at first glance, the EFF says this is often used to enhance penalties for crimes which are charged in the same indictment, negating the deterrent effect. Under the CFAA as it exists right now, penalties stack up very quickly because one action can trigger multiple parts of the same legislation. Instead, the EFF wants to clarify the language of the statute to specify actions into discernable crimes. Finally, the EFF says many of the sentencing requirements in the CFAA are simply too harsh. They advocate charging many of the less meaningful crimes within the statute as misdemeanors.

I think technology legislation has to walk a narrow line. It needs to remain specific enough that the law does not seem opaque as it’s written or capricious as it’s implemented, but broad enough to remain applicable as the technology it governs changes. The EFF’s proposed changes are certainly a step in the right direction, and represent a huge improvement on the CFAA as it exists now.
This illustration shows how asymmetric cryptography allows Alice to receive encrypted messages from anyone, which only she can read. Alice can do this by publishing her public key for anyone to use, but keeping her private key secret so only she can decrypt the messages which were encrypted with her public key.

© ConsenSys 2016


Duane, James. 2012.“Don’t Talk to the Police,” Regent University School of Law. (https://www.youtube.com/watch?v=d-7o9xYp7eE&feature=youtu.be)


