CMPSCI 590F Digital Forensics Assignment 6: Search, Possession, NITs

Vinitra Ramasubramaniam

March 8, 2017

1 US v. Tucker is a case discussed in articles that were assigned reading. The appeals court's decision is here: http://caselaw.findlaw.com/us-10th-circuit/1003230.html. In that case, investigators were able to search Tucker's home without a search warrant, serving as an example of one of the many exceptions to the protections offered by the Fourth Amendment's prohibition of unreasonable search and seizure (of our homes, among other places). To obtain a search warrant from a court, the government needs to meet the "probable cause" standard. (4 points each)

1.a What was the reason that officers didn't require a search warrant?

"Reasonable suspicion is enough to conduct a search of a parolee's home when the parolee is subject to a search condition in his parole agreement. For the same reasons, a warrant is not required in a parole search. The fact that Tucker was on parole and the officers had reasonable suspicion from Groneman's tip about Tucker's parole violation and because Tucker had agreed to search conditions in his parole, the officers did not require a search warrant."

1.b In the decision, the court reviews the difference between "reasonable suspicion" and "probable cause". What definitions and distinctions does that court make between the two concepts?

"Reasonable suspicion is a less demanding standard than probable cause. While probable cause means 'a fair probability that contraband or evidence of a crime will be found,' reasonable suspicion is merely a particularized and objective basis for suspecting criminal activity. To determine whether the investigating officers had reasonable suspicion, we consider both the quantity of information possessed by law enforcement and its reliability. Both factors must be viewed under the totality of the circumstances. When the officers' information comes from an informant, reliability may be assessed by viewing 'the credibility or veracity of the informant, the basis of the informant's knowledge, and the extent to which the police are able independently to verify the reliability of the tip.' Reasonable suspicion may exist, however, on information less reliable than that needed to establish probable cause."

1.c Tucker argued that even if the search of his home was permissible, the search of his computer was not according the decision in US v. Carey. What was the specific situation in Carey where a search was said to not be permissible?

"In Carey, the defendant was suspected of selling illegal drugs. After an officer threatened to obtain a search warrant for the defendant's house unless he consented to a search, the defendant consented to a search of the 'premises and property' located at a particular address. The searching officers found two computers they believed contained evidence of drug dealing and seized them. The police obtained a warrant to search the computers for evidence of distribution of drugs. While searching the computers, however, the officers found child pornography. This court held that the search could not be justified by the defendant's consent to search his house. As emphasized by the concurrence, our conclusion depended on the specific facts of the case, including the language of the consent agreement and the discussions held between the defendant and police officers. After examining the relevant facts,

which indicated that the defendant and the officer seeking consent were discussing a search for drugs, we concluded that the defendant did not consent to a search of his computer for child pornography."

1.d What was the court's decision regarding Tucker's claim for the subquestion above, and why was it the same or different from the decision in Carey?

"The search of Tucker's computer is distinguishable. The terms of his parole agreement are much broader. The agreement allowed parole officers to 'search my person, residence, vehicle or any other property under my control to ensure compliance with the conditions of my parole.' Thus, by its own terms, the parole agreement authorized a search of any of Tucker's property, including the computer. The parole agreement also prohibited Tucker from possessing or viewing 'any material exploiting children or depicting unconsensual sex acts or acts involving force or violence.' Therefore, unlike the consent agreement in Carey, which we interpreted as consent to a search for drugs and not child pornography, Tucker's parole agreement expressly allowed parole officers to search for any evidence that Tucker violated parole conditions by possessing or viewing child pornography."

1.e According to the Tucker decision, what is the "plain-view doctrine" for exceptions to search warrants, and what specific conditions must be met for it to apply?

"Normally, items to be seized pursuant to a warrant search must be particularly described in the warrant. We assume without deciding that the same rule applies in the parole search context. One exception to this requirement, however, is the plain-view doctrine. Under that exception, law enforcement may seize items not named in the warrant when three conditions are met. First, the seizing officer must not have 'violated the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed.' Second, the item must be in plain view and its incriminating character must be 'immediately apparent.' In other words, upon viewing the object, the officer must at that moment have probable cause to believe the object to be con-

traband or evidence of illegal activity. Finally, the officer must have a lawful right of access to the object."

2 (6 points) Ty Howard's article categorized six indications of contraband possession used by courts when deciding cases. What are they?

The six indications of contraband possession used by courts when deciding cases are:

1. The defendant's knowledge of the contraband
2. The defendant's destruction of the contraband
3. The defendant's manipulation of and control over the contraband
4. The defendant's actions to seek out and obtain the contraband
5. The amount of contraband found
6. Any other extraneous, relevant evidence

3 (10 points) Given the options discussed in the Howard and Marin articles, in your opinion, what is the most defensible and fair definition of "knowing possession" that should be applied by a court towards a criminal case? Defend it as such. (Keep in mind, it's perhaps too easy to select a definition when you have an implicit assumption of guilt in your mind for your possessor, especially given the crime considered in Howard and Marin. Try considering your definition pretending that you are in a regime where possessing something you find acceptable is illegal - perhaps a document criticizing that regime. Or simply consider that in some jurisdictions, penalties amount to life in prison, and that's a heavy burden for making a mistake.

In my opinion, a fair and defensible definition of "knowing possession" is being aware about or knowingly having control over the contraband item. The term "knowingly or being aware about" requires further explanation. I believe that if you accidentally possess or gain control of the contraband item, then this doesn't qualify for "knowing possession" as you had control but you did not seek to obtain control. If you surrender or destroy the contraband item, immediately after you gain control of it, this shows that you didn't seek to gain control or possess it. If one seeks to obtain control of a contraband item, that shows motivation to possess which indicates "knowing possession".

4 (6 points) Hennessey and Weaver propose a set of eight questions that courts should address when evaluating a NIT. Which of these questions describe circumstances where the operation of the exploit code could be material to the defense?

The following questions describe circumstances where the operation of the exploit code could be material to the defense:

1. Did the NIT seize additional information from the defendant?s system and send it to a different system on the internet?

2. Did the search conducted by the NIT exceed the scope of the warrant without seizing information?

3. Did the NIT introduce additional weaknesses to the defendant?s computer?