STATE OF NEW YORK
ERIE COUNTY COURT

THE PEOPLE OF THE STATE OF
NEW YORK

v.

[redacted]

D.A. Legacy No. [redacted]
Ind File No. [redacted]

MEMORANDUM OF LAW

[redacted].
Attorney at Law
[redacted]

Hon. Susan M. Eagan

Erie County District Attorney
25 Delaware Ave.
Buffalo, NY 14202

Mr. [redacted] is charged in this indictment with burglary in the first degree (Penal Law § 140.30[2]), and robbery in the first degree (Penal Law § 160.15[3]). This memorandum of law is submitted in support of his motion to suppress the data retrieved from his cellular phone. A hearing on the motion was held before this Court on [redacted] and [redacted].

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" (US Const Amend IV; NY Const Art I, § 12). Because the search of Mr. [redacted] cellular phone was conducted without a warrant, suppression is required.

Statement of Facts

A violent home invasion was alleged to have occurred at [redacted] in the Town of Amherst on [redacted]. After interviewing the alleged victim, William LaPorta, the defendant, and co-defendant [redacted], were developed as suspects. Amherst Police Detective [redacted] also believed that a black Mazda, belonging to [redacted], was involved. [redacted] was interviewed on [redacted] (People's Exhibit 1). She acknowledged that defendant would use her vehicle (H1 15). Subsequently, a search warrant for her vehicle was obtained (H1 8-29).

On [redacted], the vehicle was stopped, with Nelson in it, and the warrant was executed (H2 19). In the vehicle, it is claimed that work gloves, a Dollar Tree receipt for zip-ties, and a cracked cellular phone were recovered (H1 19;

People's Exhibits 4-6). The items were seized as evidence (H1 21-22). When asked if the phone was abandoned property, [redacted] said that it could be (H2 18).

The phone was provided to Officer [redacted], of the Technical Support Unit. The phone did not have a Subscriber Information Module (SIM) card in it and could not access a mobile network. The touchscreen was cracked and did not work. When plugged in, the phone's backlighting would engage, but it was not clear that the phone was charging (H2 43-45). After other testing was performed on the phone, [redacted] took the phone to the laboratory on [redacted]. The phone was hooked up to GreyKey, a Secret Service device. According to [redacted], "GreyKey will interrogate the device, and then will immediately initiate what it's programmed to do, which again is manufacturer proprietary stuff" (H2 57). Specifically, it extracts data (id.). [redacted] explained that the extraction commenced on [redacted] because there was a possibility that data could be overwritten (H2 53-54).

The defendant was arrested and interviewed on [redacted] (H1 22; People's Exhibit 2). Following *Miranda* warnings, the defendant spoke to [redacted] briefly, before invoking his right to counsel (H1 23).

I. Data search demands a warrant

In *Riley v California* (573 U.S. 373, 385 [2014]) the Supreme Court observed that cellular phones, "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy" (*Riley*, at 385). They contain a "digital record of nearly every aspect of our lives – from the mundane to the intimate"

(*Id*., at 395). Accordingly, they held that incident to arrest, the police may lawfully seize a cellular phone on a defendant's person, but they are still required to obtain a warrant *before* searching digital information contained on that phone (*Id*., 401-403).

The proposition applies with equal force here. The defendant's phone was lawfully seized pursuant to the execution of a search warrant for [redacted]s car. But [redacted] insists that the police may not search the data contained on that phone without a warrant. Saliently, the warrant for [redacted] car contained no language concerning the defendant's phone, or its contents.

Ultimately, the police did obtain a warrant for the phone. They did so five days after they searched it. That search should not be tolerated.

The People will undoubtedly argue that they did not search the phone prior to obtaining the warrant. That claim will hinge on testimony -- elicited from [redacted] and detective [redacted] (H2 59, H336) -- that they did not view the extracted data until [redacted].

In *People v Hackett* (166 AD3d 1483 [4th Dept 2018]) officers sent a text message to a number they believed was defendant's during his arrest. They observed that the defendant's phone received a message moments later. They did so before they obtained a search warrant. The defendant argued that this pre-warrant intrusion violated [redacted]. The Appellate Division rejected his claim. [redacted], they noted, does not forbid "officers from sending text messages to a defendant, making observations of the defendant's cell phone, or even manipulating the

phone to some extent upon a defendant's arrest" (*Hackett*, at 1484). Under that reasoning, it would be permissible for law enforcement, as they did here, to observe the physical damage to the phone screen, see if the touch screen worked, and arguably plug it in to determine if would charge. Here, though, law enforcement did a good deal more. For sure, plugging Mr. [redacted] phone into proprietary Secret Service software for the purpose of interrogating and extracting its contents does not fall within the understood meaning of manipulation "to some extent."

The decision in *Hackett* also rested on the record which showed that the police never "opened or manipulated the phone to get inside to retrieve data prior to obtaining a search warrant" (*Id.*, at 1484). But this is exactly what law enforcement did here. Every aspect of Mr. [redacted] life was pulled from his phone, five days before the police sought a warrant.

That the police did not, as they claim, review the extraction until after they obtained the warrant is of no moment. Initially, the language in *Hackett* does not endorse this analysis. Additionally, consider a blindfolded police officer bursting into your home this evening. Even the most shameless advocate would not argue that no 4th amendment violation occurred simply because the officer's sight was compromised.

People have put forth no evidence of abandonment.

The defendant does not contest the legality of any historical cell site data obtained by law enforcement (*People v Taylor*, 158 AD3d 1095 [4th Dept 2018]). .

The defendant does not contest the voluntariness of his statements made prior to his invocation of the right to counsel.

Data obtained from [redacted] cellular phone ought to be suppressed.

[redacted]

[redacted]
Buffalo, New York