

COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

---

No. SJC-11793

---

COMMONWEALTH OF MASSACHUSETTS,

Appellee,

v.

DENIS DORELAS,

Defendant-Appellant.

---

APPEAL FROM A JUDGMENT OF THE SUFFOLK SUPERIOR COURT

---

**BRIEF OF AMICUS CURIAE, AMERICAN CIVIL  
LIBERTIES UNION OF MASSACHUSETTS**

---

Robert E. McDonnell, BBO #331470  
robert.mcdonnell@morganlewis.com  
John Frank Weaver, BBO #673374  
john.weaver@morganlewis.com  
Arcangelo S. Cella, BBO #690438  
arcangelo.cella@morganlewis.com  
**MORGAN, LEWIS & BOCKIUS LLP**  
One Federal Street  
Boston, MA 02110-1726  
617.341.7700  
Attorneys for Amicus Curiae

Matthew R. Segal, BBO #654489  
MSegal@aclum.org  
Jessie J. Rossman, BBO #670685  
JRossman@aclum.org  
Mason Kortz, BBO #691257  
MKortz@aclum.org  
ACLU of Massachusetts  
211 Congress Street  
Boston, MA 02110  
617.482.3170

## TABLE OF CONTENTS

	Page
I. INTEREST OF <u>AMICUS CURIAE</u> .....	1
II. ISSUE PRESENTED .....	2
III. SUMMARY OF ARGUMENT .....	2
IV. ARGUMENT .....	6
A. Introduction .....	6
B. Probable Cause To Search a Smartphone For One Type of File Cannot Justify Searching the Entire Smartphone .....	12
1. The Particularity Requirement is Especially Important in Cases Involving Smartphones .....	12
2. Smartphones Are Not Mere Containers .....	18
3. The Warrant in this Case Was Not Sufficiently Particularized .....	22
C. The Police Possessed the Tools to Conduct a Less-Intrusive, Targeted Search. They Failed, However, to Resist the Urge to Rummage .....	27
D. Smartphones Also Deserve Heightened Protection Because They Contain Constitutionally Protected Speech and Associational Information .....	39
V. CONCLUSION .....	43
ADDENDUM	

## TABLE OF AUTHORITIES

Page (s)

### **Cases**

<u>Andresen v. Maryland</u> , 427 U.S. 463 (1976) .....	21
<u>Bery v. City of New York</u> , 97 F.3d 689 (2d Cir. 1996) .....	40
<u>Boyd v. United States</u> , 116 U.S. 616 (1886) .....	34
<u>Commonwealth v. Augustine</u> , 467 Mass. 230 (2014) .....	1
<u>Commonwealth v. Balicki</u> , 436 Mass. 1 (2002) .....	12, 13
<u>Commonwealth v. Dane Entertainment Services</u> , <u>Inc.</u> , 389 Mass. 902 (1983) .....	40
<u>Commonwealth v. McDermott</u> , 448 Mass. 750 (2007) .....	35, 36, 37
<u>Commonwealth v. Rousseau</u> , 465 Mass. 372 (2013) .....	1
<u>Commonwealth v. Snyder</u> , 413 Mass. 521 (1992) .....	22
<u>Commonwealth v. Toledo</u> , 402 Mass. 355 (1988) .....	13, 14
<u>Commonwealth v. Upton</u> , 394 Mass. 363 (1985) .....	13, 22, 34
<u>Entick v. Carrington</u> , 19 How. St. Tr. 1029 (C.P.) (Eng.) (1765) .....	34
<u>Groh v. Ramirez</u> , 540 U.S. 551 (2004) .....	12

<u>Larsen v. Fort Wayne Police Dept.,</u> 825 F. Supp. 2d 965 (N.D. Ind. 2010) .....	40
<u>Marron v. United States,</u> 275 U.S. 192 (1927) .....	24
<u>Maryland v. Garrison,</u> 480 U.S. 79 (1987) .....	13, 25
<u>Messerschmidt v. Millender,</u> 132 S. Ct. 1235 (2012) .....	25, 26
<u>NAACP v. Alabama,</u> 357 U.S. 449 (1958) .....	42
<u>Preventive Med. Associates, Inc. v.</u> <u>Commonwealth,</u> 465 Mass. 810 (2013) .....	37
<u>Riley v. California,</u> 134 S.Ct. 2473 (2014) .....	<i>passim</i>
<u>Stanford v. Texas,</u> 379 U.S. 476 (1965) .....	39, 40
<u>United States v. Barbuto,</u> U.S. Dist. Ct., No. 2:00CR197K, slip op. (D. Utah. April 12, 2001) .....	21
<u>United States v. Carey,</u> 172 F. 3d 1268 (10th Cir. 1999) .....	18, 21
<u>United States v. Comprehensive Drug Testing,</u> <u>Inc.,</u> 621 F.3d 1162 (9th Cir. 2010) .....	38
<u>United States v. Falso,</u> 544 F.3d 110 (2d Cir. 2008) .....	26
<u>United States v. Flores-Lopez,</u> 670 F. 3d 803 (7th Cir. 2012) .....	18, 20
<u>United States v. Kirschenblatt,</u> 16 F.2d 202, 203 (2nd Cir. 1926)) .....	19
<u>United States v. Lucas,</u> 640 F.3d 168 (6th Cir. 2011) .....	20



<u>United States v. Mann</u> , 592 F.3d 779 (7th Cir. 2010) .....	21
<u>United States v. Walser</u> , 275 F.3d 981 (10th Cir. 2001) .....	21
<u>United States v. Winn</u> , U.S. Dist. Ct., No. 14-CR-30169-NJR, slip op. at 9-10 (S.D. Ill. Feb. 9, 2015), <u>appeal filed</u> , No. 15-1500 (7 <sup>th</sup> Cir. March 9, 2015) .....	<i>passim</i>
<u>Watkins v. United States</u> , 354 U.S. 178 (1957) .....	42
<u>Wilkes v. Woods</u> , Lofft 1, 19 How. St. Tr. 1153, 98 E.R. 489 (1763) .....	9
<u>Zurcher v. Stanford Daily</u> , 436 U.S. 547 (1978) .....	40
<b>Constitutional Provisions and Statutes</b>	
First Amendment to the United States Constitution .....	40, 42
Fourth Amendment to the United States Constitution .....	<i>passim</i>
Article 14 of the Massachusetts Declaration of Rights .....	<i>passim</i>
G.L. c.265, §15 .....	8
G.L. c.265, §15B .....	8
<b>Other Authorities</b>	
Cellebrite, Wikipedia, at <a href="http://en.wikipedia.org/wiki/Cellebrite">http://en.wikipedia.org/wiki/Cellebrite</a> (last viewed Mar. 25, 2015) .....	29
Cellebrite Mobile Synchronization Ltd., Brochure, UFED TK: The Rugged Mobile Forensic Tactical Kit, at <a href="http://www.cellebrite.com/images/stories/brochures/UFED-TK-web.pdf">http://www.cellebrite.com/images/stories/brochures/UFED-TK-web.pdf</a> (last viewed Mar. 27, 2015) .....	28, 29

Cellebrite Mobile Synchronization Ltd., Universal Forensic Extraction Device User Manual, June 2009, at <a href="https://www.cellebrite.com/images/stories/support%20files/UFED-UserManual-v4b.pdf">https:// www.cellebrite.com/images/stories/support% 20files/UFED-UserManual-v4b.pdf</a> (visited March 25, 2015) .....	29, 31
Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 542 (2005) .....	19
Ritchie, History of iPhone: Apple Reinvents the Phone, iMore (Aug. 22, 2014), at <a href="http://www.imore.com/history-iphone-2g">www.imore.com/history-iphone-2g</a> (last viewed Mar. 27, 2015) .....	36

## I. INTEREST OF AMICUS CURIAE

The American Civil Liberties Union of Massachusetts (ACLUM) is a statewide civil rights and civil liberties organization which has long worked to promote, defend, and to educate citizens about the privacy, property rights, due process, and civil rights protected by the Fourth Amendment of the United States Constitution and Article 14 of the Massachusetts Declaration of Rights. ACLUM has participated as amicus curiae in numerous Fourth Amendment and Article 14 cases in this Court. See, e.g., Commonwealth v. Augustine, 467 Mass. 230 (2014) (direct representation arguing that the Fourth Amendment and Article 14 require a warrant to obtain cell phone site location information); Commonwealth v. Rousseau, 465 Mass. 372 (2013) (amicus arguing that GPS monitoring of a vehicle constitutes a search and seizure of all the vehicle's occupants). It has a strong and longstanding interest in the practices and procedures governing the use of search warrants, and it has been diligently examining and evaluating the application of those practices and procedures to developing technologies. ACLUM's affiliated national organization, the American Civil Liberties Union based

in New York, participated as an amicus curiae in Riley v. California, 134 S.Ct. 2473 (2014), in which the Court ruled against the warrantless search of smartphones incident to arrest. The captioned case presents the Supreme Judicial Court with a case and controversy putting at issue the proper rules and procedures to be followed in the wake of Riley.

## II. ISSUE PRESENTED

The Court's solicitation of amicus briefs, SJC-11793, invited submissions as follows:

Whether, when a search warrant is sought to search a "smart phone," probable cause is needed for each of the distinct file types to be searched, i.e., text messages, photographs, e-mails, etc., and whether the warrant must be particular in terms of the specific types of files to be searched.

## III. SUMMARY OF ARGUMENT

The advance of technology does not excuse the need to adhere to the probable cause and particularity principles established by the Fourth Amendment to the United States Constitution and by Article 14 of The Massachusetts Declaration of Rights. Warrants to search smartphones should permit police officers to

examine only the specific files for which probable cause exists. The technology to allow the police to comfortably limit their searches of smartphones to the files for which probable cause exists is already available. Unfortunately, that technology was misused in the Dorelas investigation because the police had improperly obtained a general warrant. The courts, magistrates and police should not rely upon "the container analogy" when reviewing, issuing, or obtaining warrants to search smartphones. These pocket-sized computers contain such a quantity and quality of personal information that they are entitled to the same safeguards applied to the search of houses, offices and personal effects.

Each file in a smartphone is capable of being stored in a different way and implicating privacy interests for different sets of reasons. Meanwhile, the rapid advance of technology has provided the police with the means to organize and retrieve data with increasing focus and precision. In Riley v. California, 134 S.Ct. 2473 (2014), the volume, variety, and sensitivity of the information either stored in the smartphone or stored remotely (in "the cloud") and accessed through the smartphone led the

Court to conclude that the privacy interests involved in smartphone searches "dwarf" those examined in past cases, when only limited information contained in a finite space was involved. The Court rejected the "container analogy" as a basis for justifying the warrantless search of a smartphone. In the wake of Riley, at least one federal court has ruled in favor of a file-based search of smartphones. The police may search only the specific files for which probable cause to search has been established. Police must identify where in the smartphone they want to search and what they are looking for when requesting a warrant, just as they would have to if they wanted to search a person's home. Further reliance on the container analogy to search smartphones will result in the issuance of general warrants, and after-the-fact rationalizations for overbroad searches.

The police have the ability to search smartphones with precision, and they should be held to a high standard in order to preserve the privacy rights protected by the Fourth Amendment and Article 14. The Universal Forensic Extraction Device (UFED) used by the police in the Dorelas investigation gave them the ability to limit the search of the smartphone to the

files for which probable cause existed: telephone calls and text messages. Perversely, the police misused the technology to improperly expand the search beyond the bounds of probable cause and particularity. In light of technical advances like the UFED, the police should be required to explain to the magistrate in the warrant application the means and methods that will be used to search for particular items located in specific files in smartphones.

In addition to containing large amounts of data revealing the most private aspects of a person's life, smartphones also contain expressive and associational materials. In keeping with Supreme Court precedent, warrant applications seeking to search smartphones containing expressive or associational information should be subjected to "exacting scrutiny." The police should not be allowed to indiscriminately examine a smartphone file that may contain thousands of photographs without undergoing some form of heightened scrutiny. At a minimum, a magistrate should require the police to demonstrate that there is little to no probability that they are invading a form of protected expression. The risk of invading expressive and associational rights requires magistrates to give

smartphone search warrant applications an exacting scrutiny that demands strict compliance with the twin mandates of probable cause and particularity.

#### **IV. ARGUMENT**

##### **A. Introduction**

This case presents an opportunity to apply traditional search and seizure safeguards to 21<sup>st</sup> century technology. It is well established that search warrants must be based upon probable cause to believe that particular items will produce evidence of a crime and be found in particularly described locations. As human ingenuity advances, as inventions multiply, or as time simply passes, these fundamental protections against unreasonable searches and seizures can and must endure. Accordingly, warrants to search smartphones should permit police officers to examine only the specific files for which probable cause exists. Merely because modern technology makes it possible to store a trove of personal, private information in a pocket-sized computer does not make it tenable for officers to rummage at will through the entire trove when probable cause exists to examine only a limited subset of the information. Unfortunately, unconstitutional rummaging is what



happened here, even though the police possessed a data-extraction device that enabled them to limit their search to files for which probable cause existed.

In this case, the police arguably had probable cause to believe that call records or text messages on defendant Denis Dorelas's smartphone would contain evidence of unlawful threats. With respect to those items, the police did traditional investigative work. They interviewed a witness who said "that Mr. Dorelas received a phone call and started arguing with the caller on the phone" immediately before a gunfight. See Aff. Supp. Appl. for Search Warrant, ¶ 6 (Aff.), Record Appendix (R.A.) 105. They allegedly learned that Dorelas had been "receiving threatening phone calls and threatening text messages on his phone." Id. ¶ 7 (R.A. 106). And they heard that "Denis has been getting a lot of telephone threats because he owes money to people." Id. ¶ 8 (R.A. 106).

Despite the narrow specificity of that evidence, the Commonwealth sought, and a magistrate approved, a warrant to search Dorelas's phone for text messages, call records, and a raft of other quintessentially private information. The warrant permitted officers to

sweep up, among other items, "saved and deleted photographs," "mobile internet browser," and saved, draft, or deleted email messages. R.A. 108. The materials supporting the warrant application, however, offered no facts to justify collecting such a broad range of file types. Those materials, for example, demonstrated no nexus between any crime and any photographs in Dorelas's smartphone. And, notwithstanding the Commonwealth's arguments to this Court, those supporting materials did not present even a whiff of police expertise suggesting that modern-day criminals, à la Bonnie and Clyde, are prone to take self-portraits of themselves and their firearms. Instead, the investigating officer all but conceded that he was seeking the warrant for the purpose of investigating crimes unrelated to the concrete evidence of threats via phone calls and text messages: assault and battery with a dangerous weapon in violation of G.L. c.265, §15B, and assault with intent to murder in violation of G.L. c.265, §15. Aff. ¶ 2 (R.A. 105).

The result of this effort was, in effect, a general warrant. Such a warrant should not be permitted now because, in this Commonwealth, it has

never been permitted. There is nothing about modern technology that justifies a drift toward general warrants. The opposite, in fact, is true. Technology exists to enable police to conduct constitutional searches limited to information for which probable cause exists.

Two-hundred-fifty-two years ago, in an infamous case that no doubt influenced the Framers of the Fourth Amendment and Article 14 of the Declaration of Rights, counsel for the victim of a general warrant urged the English Court of Common Pleas to undo the mischief of an improper and invasive search and "to embrace this opportunity . . . of instructing those great officers in their duty, [by] . . . erect[ing] a great sea mark, by which our State pilots might avoid, for the future, those rocks upon which they now lay shipwrecked." Wilkes v. Woods, Lofft 1, 19 How. St. Tr. 1153, 98 E.R. 489 (1763). Today, the risk of search-and-seizure shipwreck arises from the ease with which governments can leverage technology, and smartphones in particular,<sup>1</sup> to invade private lives. A smartphone is home, office, and off-site archive

---

<sup>1</sup> See DeGusta, Are Smartphones Spreading Faster Than Any Technology in Human History?, MIT Tech. Rev. (May 9, 2012).

rolled into one. It is a computer, diary and camera. It is a beacon capable of revealing where we have been, where we are, and where we intend to go.

For this reason, and as the Supreme Court has already explained, a traditional "container analysis" -- whereby the government can search all of the contents of a container without describing them with particularity -- does not adequately protect the expectations of privacy that citizens have in their smartphones. Riley v. California, 134 S. Ct. 2473 (2014). People use smartphones to create a "digital record of nearly every aspect of their lives - from the mundane to the intimate." Id. at 2490. The amount of data on a smartphone can easily exceed the amount of data that could possibly have been found inside a home during the pre-digital era. See id. at 2493. In reality, each file type on a smartphone is the equivalent of a different house or office on a large city block. Probable cause to search one office does not provide a basis to invade and rummage the neighboring office. Thus, as one federal district court has already ruled, those simple facts mean that a warrant to search a smartphone should meet the more exacting particularity requirements that are routinely

applied to searches of homes, offices, and other locations containing comparable types of private information. United States v. Winn, U.S. Dist. Ct., No. 14-CR-30169-NJR, slip op. at 9-10 (S.D. Ill. Feb. 9, 2015), appeal filed, No. 15-1500 (7<sup>th</sup> Cir. March 9, 2015).

Critically, the Commonwealth not only should conduct particularized searches of smartphones based on probable cause, it also can do so. The very device that the police used to extract data from the Dorelas smartphone reveals that the police willfully targeted the Defendant with electronic buckshot when they could have conducted a constitutional search with laser-like precision. This Court must hold the Commonwealth to its well-established constitutional obligations.

A contrary holding would send the wrong message to the police and the public. It will tell the police that having gained access to one or two smartphone files upon a showing of probable cause, they are at liberty upon a "bare suspicion" to run amuck through the remaining files. And it would tell citizens that their expectations of privacy under Article 14 and the Fourth Amendment have been badly eroded. Instead, this Court should make clear that a warrant application to

search a cell phone must list with particularity the specific files in which there is probable cause to believe evidence of a crime is stored.

The evidence supporting the warrant application pointed to two, but only two, possible sources of evidence: call records and text messages. The police knew where these items were likely to be found on the phone, and they also knew that they possessed the means -- a Cellebrite "Universal Forensic Extraction Device," or "UFED" -- to limit their search to those items. See R.A. at 106. The police should have disclosed to the magistrate their ability to pinpoint relevant files on the smartphone without rummaging through the entire device. This they failed to do.

**B. Probable Cause To Search a Smartphone For One Type of File Cannot Justify Searching the Entire Smartphone.**

**1. The Particularity Requirement is Especially Important in Cases Involving Smartphones.**

Search warrants must be based upon particularly described places to be searched and things to be seized. See Groh v. Ramirez, 540 U.S. 551, 557 (2004); Commonwealth v. Balicki, 436 Mass. 1, 7 (2002). That requirement serves as a safeguard against general exploratory rummaging by the police through a person's

belongings. Id. Accordingly, a valid search warrant must rest on "a substantial basis for concluding that any of the articles described in the warrant are probably in the place to be searched." Commonwealth v. Upton, 394 Mass. 363, 370 (1985). To prevent "the wide-ranging exploratory searches the Framers intended to prohibit," the government must "establish probable cause as to each area and item to be searched. Maryland v. Garrison, 480 U.S. 79, 84 (1987) (authorization of search warrant must be limited "to the specific areas and things for which there is probable cause to search, [a] requirement ensur[ing] that the search will be carefully tailored to its justifications").

These principles have long meant that officers seeking or executing a search warrant can intrude only into the areas justified by the materials supporting the warrant. For example, in Commonwealth v. Toledo, 402 Mass. 355 (1988), two witnesses stated that the defendant sold cocaine in an apartment described as "the front apartment on the 2<sup>nd</sup> floor directly above No. 17" at 50C Memorial Road. The police included those statements in the affidavit used to obtain a warrant to search "the front apartment on the 2<sup>nd</sup> floor

above apartment #17 located at 50C Memorial Road." However, the resulting search extended to an additional apartment not identified in the affidavit or warrant. There, the police found evidence used against the defendant. This court affirmed the lower court's decision to suppress that evidence. Id. at 361.

These principles take on a special role in protecting "the privacies of life" when the police search a smartphone. The right to be free from general warrants developed when no information was stored digitally, and thus all recorded private information took up tangible space. Smartphones, however, can contain abundant information in a negligibly small space,<sup>2</sup> and they can remotely access information stored in other locations -- including the home -- throughout the physical world. Smartphones have numerous files, databases, and file areas where data, documents, information, and items can be stored. R.A. at 45. Each one is capable of being stored in a different way and implicating privacy interests for different sets of

---

<sup>2</sup> A popular type of iPhone features 64 GB of storage, which is large enough for a person to shoot and carry over 70 hours of private video in her pocket. Price, What's an iPhone or iPad's True Storage Capacity?, Macworld (April 14, 2014).



reasons. Meanwhile, the rapid advance of technology has provided the police with the means to organize and retrieve data with increasing focus and precision.

These facts of modern life led to the unanimous decision in Riley, where the Supreme Court held that police officers may not search a smartphone based on having probable cause to arrest its owner. Instead, they must "get a warrant." 134 S. Ct. at 2495.

The Supreme Court's reasoning in Riley has clear implications for the kind of warrant that officers must get. The Court recognized that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." 134 S. Ct. at 2488-2489. The Court observed that "a cell phone search would typically expose to the government far more than the most exhaustive search of a house[.]" Id. at 2491. The volume, variety, and sensitivity of the information either stored in the smartphone or stored remotely (in "the cloud") and accessed through the smartphone led the Court to conclude that the privacy interests involved in smartphone searches "dwarf" those examined in past cases, when only limited information contained in a finite space was involved. Id.

Applying this reasoning, a federal court has ruled that a warrant to search all content on a device is invalid when the police fail to demonstrate probable cause that everything on the phone is evidence. Winn, slip op. at 10. In that case, witnesses alleged that the defendant had been pointing his smartphone in the direction of young girls at a swimming pool and either photographing or videotaping them. But, as in this case, the police in Winn did not tailor a warrant request to the types of files as to which they had probable cause. Instead, they copied a template seeking authorization for the broadest search possible, a search encompassing an expansive range of data potentially relevant to any case.

The district court held that this approach violated the Fourth Amendment because it ran afoul of the particularity requirement. The court reasoned that, because the officer obtained the warrant based on accusations about Winn's behavior at the swimming pool, the officers had probable cause only to investigate the crime of public indecency. But "only two categories of data could possibly be evidence of [that crime]: photos and videos" (emphasis added). Id. at 9. Indeed, "the narrative portion of the complaint

did not even mention [other] categories of data." Id. Thus, the court explained, officers could not permissibly rely on a template that failed to differentiate one category from another:

Templates are, of course, fine to use as a starting point. But they must be tailored to the facts of each case. This particular template authorized the seizure of virtually every piece of data that could conceivably be found on the phone. . . . Obviously, the police will not have probable cause to search through and seize such an expansive array of data every time they search a cell phone" (emphasis added).

Id., citing Riley, 134 S. Ct. at 2491.

The court in Winn also refused the prosecution's invitation to speculate as to whether the alleged photos or videos could have been moved to other files by being attached to a text message or email or by internet upload. The court explained that "[t]he police cannot rationalize a search *post hoc* on the basis of information they failed to set forth in their warrant application to a neutral [judge].'" Id., quoting Messerschmidt v. Millender, 132 S. Ct. 1235, 1257 n.8 (2012).

As to the files for which no probable cause existed, the court ruled that the police should have established probable cause as to each type of data.

Their failure to do so at the time they applied for the warrant was fatal to its validity:

The bottom line is that if Detective Lambert wanted to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to Winn's criminal activity, and he did not do so. Consequently, the warrant was overbroad, because it allowed the police to search for and seize broad swaths of data without probable cause to believe it constituted evidence" (emphasis added).

Id. at \*10.

## **2. Smartphones Are Not Mere Containers.**

The Commonwealth's argument in this case, which directly contradicts the reasoning of *Riley* and the holding of *Winn*, essentially treats a smartphone just like any other "container of information." United States v. Flores-Lopez, 670 F. 3d 803, 805 (7<sup>th</sup> Cir. 2012); Comm. Br. at 35-36, 39-40. That approach risks "oversimplify[ing] a complex area of Fourth Amendment doctrines and ignor[ing] the realities" of data storage in cell phones. United States v. Carey, 172 F. 3d 1268, 1275 (10th Cir. 1999) (quoting Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994)). In truth, smartphones are not mere containers. They are more like entire virtual buildings because they are "akin

to a vast warehouse of information." Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005).

Indeed, not only is it misleading to describe smartphones as containers, even calling them phones is a "misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." Riley, 124 S. Ct. at 2489. There, the Supreme Court cited Learned Hand, who wrote that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything that may incriminate him." 134 S. Ct. at 2490-91. (quoting United States v. Kirschenblatt, 16 F.2d 202, 203 (2nd Cir. 1926)). In providing a modern response to that thought, the Riley Court wrote "If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house." 134 S. Ct., at 2491. The Court even goes so far as to skeptically compare a search of a cell phone incidental to arrest to "finding a key in a suspect's pockets and arguing that it allowed law enforcement to unlock and search a house." Id.

Thus, "[t]he potential invasion of privacy in a search of a cell phone is greater than in a search of a 'container' in a conventional sense." Flores-Lopez, 670 F. 3d at 805. Smartphones, as minicomputers, "hold so much personal and sensitive information touching on many private aspects of life" that "there is far greater potential 'for the intermingling of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.'" United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) (quoting United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001)). To protect against the intermingling of documents on a smartphone, police must identify where in the smartphone they want to search and what they are looking for when requesting a warrant, just as they would have to if they wanted to search a person's home.

Given that smartphones frequently contain the "sum of an individual's private life," Riley, 134 S. Ct. at 2489, warrants to search them should require descriptions of locations and items that are at least as particular as warrants to search computers. The Tenth Circuit has repeatedly noted that "officers conducting searches (and the magistrates issuing

warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive." Wasler, 275 F.3d at 986 (citing Carey, 172 F.3d at 1275). See also United States v. Barbuto, U.S. Dist. Ct., No. 2:00CR197K, slip op. at 5 (D. Utah, April 12, 2001) (recognizing "the important limitations on the scope of computer searches," in Carey that require "a more particularized inquiry"). Similarly, the Seventh Circuit has counseled "officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described." United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010). These requirements are consistent with the Supreme Court's instruction that when it comes to searches, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

3. The Warrant in this Case Was Not Sufficiently Particularized.

The particularity required of warrants to search a computer was not on display here. The police failed to present facts to the magistrate supplying probable cause that files other than text messages and phone calls would yield evidence of a crime. Accordingly, the warrant relied upon to search Dorelas's smartphone was invalid as to the search of files other than phone calls and text messages.

The relevant evidence presented in the affidavit consisted of the three witnesses who stated that Mr. Dorelas received "threatening phone calls and threatening text messages on his phone." R.A. at 106.

As set out in the affidavit's narrative, the police believed that those threats were evidence of a crime. Aff. ¶¶ 7-8 (R.A. 106). Thus, the police had to establish probable cause that the threatening calls and text messages would likely be found in the places that they requested authorization to search. See Commonwealth v. Snyder, 413 Mass. 521, 527 (1992); Upton, 394 Mass. at 370.



However, the police requested a much broader warrant to search. The list appearing in the warrant application contains twelve line-items:

- A. Subscriber telephone number,
- B. Electronic Serial Number, International Mobile Equipment Identity, Mobile Equipment Identifier, or identification number,
- C. Contact list, address book, calendar, and date book entries,
- D. Group list,
- E. Speed dial list,
- F. Phone configuration information and settings,
- G. Incoming, outgoing, and draft sent and deleted text messages,
- H. Saved, opened, and unopened voice mail messages,
- I. Saved, opened, unopened, draft, sent, and deleted electronic mail messages,
- J. Mobile instant message and logs, data, and contact information,
- K. Mobile internet browser history,
- L. Saved and deleted photographs and movies.

This list -- including emails, internet history, photographs, and videos -- far exceeds the potential types and locations of evidence described by the witnesses. R.A. at 106-107. The subsequent boilerplate search warrant essentially rubber-stamped the boilerplate application without due regard to the limited set of facts set forth in the Affidavit supporting the warrant application. R.A. at 108.

Such a broad list of file types and areas to search in the phone supported by such a paucity of evidence robs the warrant of the particularity

necessary under the Fourth Amendment and Article 14. It is akin to a witness telling the police that a bloody pillow is located in the master bedroom, and in response the police request a warrant to search the garage, mudroom, kitchen, first floor bathroom, living room, pantry, second floor bathroom, master bedroom, guest room, second floor bathroom, linen closet, basement, and attic. The particularity requirement "makes general searches under [search warrants] impossible and prevents the seizure of one thing under a warrant describing another." Marron v. United States, 275 U.S. 192, 196 (1927). The witnesses' statements described threatening phone calls and text messages; it should have been impossible for the police to seize photographs saved in the photograph file on Mr. Dorelas's phone.

Accordingly, the court's analysis in Winn is directly applicable here. As in Winn, the police established "probable cause to believe that only two categories of data could possibly be evidence of the crime" (emphasis added), without any mention in the narrative of the other files that they requested to search. Id. at 9. Instead, the list of files included in the Dorelas warrant, like the unmodified template

in Winn, "authorized the seizure of virtually every piece of data that could conceivably be found on the phone," without any apparent effort to tailor the list to the facts of the case. Id. See also Garrison, 480 U.S. 79, 84 (stating that a search must be "carefully tailored to its justification"). For this reason, the Dorelas warrant is overbroad. It granted the police's request to search files for which they did not establish probable cause, and therefore it is invalid. Winn, slip op. at 9-10; Messerschmidt, 132 S.Ct. at 1257 n.8.

At this point, no amount of speculation or post hoc rationalization can save the Dorelas warrant. The government attempts to dance the Limbo at great length to point out that threats may be conveyed through pictures. Com.'s Br. 27-29 (citing cases in which physical, not digital, photographs constituted threats). The Commonwealth also argues that even in the absence of a threatening picture, the actual text of a threatening message could be transferred to the photograph file by means of a screenshot. Com.'s Br. 9 n.6, 30. If the police had any information indicating that Defendant had received a threatening photograph on his smartphone and that he had stored it in his

photograph file, or that he had memorialized a text by taking a screenshot, then they should have presented it to the magistrate in the affidavit. See Winn, slip op. at 9-10; Messerschmidt, 132 S. Ct. at 1257 n.8. The ability to take a screenshot does not mean the Defendant did, and the Commonwealth is not entitled to justify a search by rank, post hoc speculation. See United States v. Falso, 544 F.3d 110, 121 (2d Cir. 2008) (no probable cause where affidavit merely recited that defendant had ability to view child pornography on Web site defendant visited, but did not state whether defendant accessed, viewed, or downloaded child pornography). The police did not even offer any "law enforcement expertise" to support the search for photographs. All of the Commonwealth's rationales have been after-the-fact and laced with speculation. Such conduct does not satisfy Fourth Amendment and Article 14 standards.

The precedent set by permitting this search is dangerous, as an affidavit indicating that there is relevant information in a particular location on a smartphone could lead to a warrant authorizing a search of all or nearly all file locations on the phone. A witness stating that a calendar appointment

contains the name of other suspects would permit the police to search personal emails, personal notes, and other private and constitutionally protected files and data on the phone. It is important for this Court to firmly establish that a warrant to search a smartphone can only be valid if it describes with particularity the items and locations on the phone to be searched.

**C. The Police Possessed the Tools to Conduct a Less-Intrusive, Targeted Search. They Failed, However, to Resist the Urge to Rummage.**

Just as the search in this case demonstrates why this Court should apply a strong particularity requirement to warrants to search smartphones, it also demonstrates that law enforcement officials can comfortably satisfy such a requirement. The police have the ability to search with precision, and they should be held to a high standard in order to preserve the privacy rights protected by the Fourth Amendment and Article 14.

The police in this case possessed a powerful, hi-tech tool to search Defendant's smartphone: the UFED. As the expert Joseph Nicholls explained to the Superior Court, the UFED is capable of extracting only phone calls and text data, without searching the photograph file area at all. Tr. at 29, 33, 45-46.

Distinguishing between areas of the phone to search is as easy as checking boxes on the UFED, so there is no practical reason for police to refuse the Fourth Amendment protection courts have begun to recognize in a person's smartphone and in each different file area of a smartphone.

The manufacturer of the UFED, Cellebrite, markets itself as "the world leader in delivering leading-edge mobile forensic solutions." Cellebrite Mobile Synchronization Ltd., Brochure, UFED TK: The Rugged Mobile Forensic Tactical Kit, About Cellebrite, at <http://www.cellebrite.com/images/stories/brochures/UFE-D-TK-web.pdf> (last viewed Mar. 27, 2015). The company claims that its "comprehensive Universal Forensic Extraction Device (UFED) is designed to meet the challenges of unveiling the massive amount of data stored in the modern mobile device. The UFED Series is able to extract, decode, analyze and report data from thousands of mobile devices, including smartphones, legacy and feature phones, portable GPS devices, tablets, memory cards and phones manufactured with Chinese chipsets." Id. Since 1999, Cellebrite has sold more than 30,000 units in 100 countries. It considers its UFED Series to be "the primary choice for forensic

specialists in law enforcement, military intelligence, corporate security and eDiscovery." Id. The UFED reportedly has:

the widest coverage available in the mobile forensics market, with the ability to extract data from nearly 8200 devices as of June 2012. These include smartphones, PDA devices, cell phones, GPS devices and table computers. The UFED can extract, decrypt, parse and analyze phonebook contacts, all types of multimedia content, SMS and MMS messages, call logs, electronic serial numbers (ESN), International Mobile Equipment Identity (IMEI) and SIM location information from both non-volatile memory and volatile storage alike, in multiple international languages including Middle Eastern and European languages. The UFED supports all cellular protocols including CDMA, GSM, IDEN, and TDMA, and can also interface with different operating systems' file systems such as iOS, Android OS, BlackBerry, Symbian, Windows Mobile and Palm as well as legacy and feature cell phones' operating systems.

Cellebrite, Wikipedia, at <http://en.wikipedia.org/wiki/Cellebrite> (last viewed Mar. 25, 2015).

Law-enforcement agencies can use the UFED to disgorge the entire contents of a smartphone. In other words, the police can perform a complete "memory dump." See Cellebrite Mobile Synchronization Ltd., Universal Forensic Extraction Device User Manual, June 2009 [hereinafter User Manual], at <https://www.cellebrite.com/images/stories/support%20files/UFED>

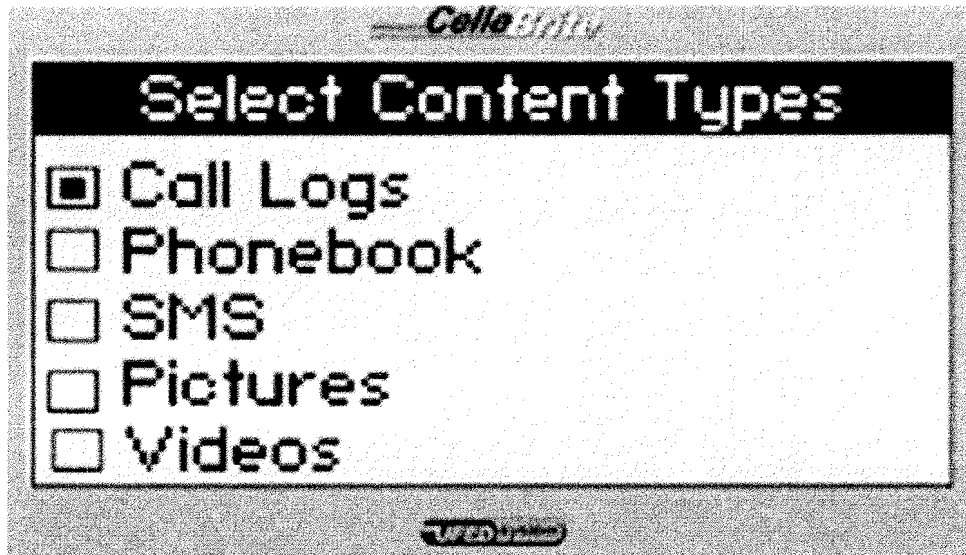
-UserManual-v4b.pdf (visited March 25, 2015) (copy attached in Appendix to this brief, pp. A. 19-79). Thus, if misused, the UFED provides the police with the means to rummage through the vast storehouse of data filed in a smartphone. Consideration of the UFED reveals the degree of risk of invasion to which personal computing devices and smartphones are exposed.

But a complete memory dump followed by unrestricted rummaging through the data is not law enforcement's only option. As explained in the User Manual, the UFED can be restricted to a targeted search. In other words, the police can apply particularity to the UFED and limit their intrusion to the material -- and only the material -- that they have probable cause to search.

The User Manual provides step-by-step instructions to limit the scope of the UFED data extraction. After setting up the UFED (in the field or the office as the case may be) and connecting it to the smartphone, Step 1 provides the option to "Extract Phone Data." User Manual, at 13. Next, the operator selects the proper manufacturer, id., and, in Step 3, identifies the proper manufacturer model, id. Steps 4,



5 and 6 continue the extraction set-up. Id. at 14-15. Step 7 provides the police with a very clear opportunity to target the search to particular kinds of data. Id. at 15.



In Step 7, the menu illustrated above appears on the UFED's screen. The operator uses this menu to "[s]elect content types to be extracted." Id. According to the manual, the UFED displays options in accordance with the capabilities that are "available in the phone." Id. The operator checks the boxes that identify the type or types of data to be extracted.

In the Dorelas investigation, the police could have and should have limited the smartphone search to "call logs" "phonebook" and "SMS." As explained at the March 11, 2013 suppression hearing, the "call logs" provided the police with the calls that Dorelas made

or received. Tr. at p. 23 line 10. In other words, checking the "call logs" box might have provided the police with information about the person or persons who were reportedly threatening Dorelas about his debts. The "phonebook" would have provided the police with the telephone contacts Dorelas had entered in his smartphone. Again, this data might have revealed evidence concerning persons who were reportedly threatening Dorelas by telephone. Assuming that the smartphone had been lawfully seized in the first place, witness interviews arguably gave the police probable cause to check the first two boxes on the UFED.

The suppression hearing also revealed that checking the "SMS" option on the UFED would have given the police access to both simple text messages and to text messages with photographs or other items attached. "SMS" stands for "simple message system." Tr. at p. 12 lines 12-17. That phrase in turn refers to a words-only text message. Tr. at p. 26 lines 15-20 ("SMS for simple messages system. . . . That refers to text messages"). Texts, however, can also have photographs attached to them on the iPhone system. (Dorelas's smartphone was either an Apple iPhone 3G or

iPhone 4. Tr. at 43-44.) The "multimedia message service" or MMS can attach "pictures, voice, video, even graphic files" to a text message. Tr. at p. 26 line 21, p. 27 line 2. The UFED software in use at the time of the Dorelas search only offered the SMS option (as in the screen illustrated above), but checking that box provided the police with both simple text messages and with text messages that included attachments such as photographs:

That was a current version at the time the extraction happened. At that point, to get MMS messages, all that was presented to the [UFED] examiner was SMS, and the software at that point, if you selected SMS as the data type you wanted to extract, it would get both text messages and MMS messages.

Tr. at p. 48 line 23, p. 49 line 4.

Limiting their search to the first three boxes on the UFED screen would have opened only the files that the police reasonably believed contained smartphone data related to the reported threats made against the Defendant. But, of course, that is not what happened here.

Instead, officers turned the key to files for which they lacked probable cause. By checking boxes 4 (photographs) and 5 (videos), the police cut their constitutional mooring lines and steered into the

murky, inadequate shoals of having only a "strong reason to suspect." Upton, 394 Mass. at 370. As that case holds, a "strong reason to suspect" does not amount to probable cause.

The police had no basis to search the Defendant's photograph file. The Warrant Affidavit, R.A. 105-107, is devoid of any basis to do so. Failing to resist the urge to rummage, the police submitted a boilerplate application. The magistrate rubber-stamped it, and issued a warrant authorizing "the secret cabinets and bureaus of [Dorelas's smartphone] . . . [to] be thrown open to the search and inspection of a messenger . . ." Entick v. Carrington, 19 How. St. Tr. 1029 (C.P.) (Eng.) (1765).<sup>3</sup>

The boilerplate warrant was a general warrant. Armed with it, the UFED operator checked the box for

---

<sup>3</sup> In Entick, the King's messengers conducted a four-hour search of Entick's home, broke open locks and doors, and seized hundreds of pamphlets. In Boyd v. United States, the Supreme Court noted that Entick "laid down . . . the very essence of constitutional liberty and security. . . . It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offense, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment." 116 U.S. 616, 630 (1886).

photographs, and also checked the box marked "videos." By checking those boxes, the police opened the door to an unreasonable search of Defendant's private life - a search that "expose[d] to the government far more than the most exhaustive search of [Dorelas's] house" Riley, supra, which -- ironically -- they had already searched. When applying to search a suspect's smartphone, the Fourth Amendment and Article 14 require the police to demonstrate probable cause for each of the files they intend to search. Riley, 134 S. Ct. at 2491. The constitutional mandates also require the Magistrate to limit the warrant with particularity to the smartphone files for which probable cause exists.

The Commonwealth cites Commonwealth v. McDermott, 448 Mass. 750 (2007), in an after-the-fact attempt to justify the police search of Defendant's photograph file. In that case, arising out of a shooting rampage at a Wakefield business, the police seized and searched the defendant's computers and storage disks. The police made a "forensic duplicate" of the computers and storage media, and then used the "EnCase" program to run a search for "approximately 250 keywords that were pertinent to the

investigation." Id. at 774. The Court ruled that the search was reasonable because the "keyword search method resulted in a cursory inspection of only approximately 750 files out of the 100,000 files . . . less than one per cent of the defendant's files." Id. at 777.

In McDermott, the police did the exact opposite of what the police did here. In McDermott, law enforcement used technology to limit the scope of the search. They used technology to narrow the search to files relevant to the crimes under investigation, and to narrow the invasion into the defendant's private life. In the Dorelas investigation, the police used technology to expand their search beyond the bounds of probable cause. Worse, they ignored the fact that the UFED gave them the means and method to keep their search within the confines of the Constitution and Article 14.

Although decided on April 13, 2007, and thus only eight years old, McDermott was decided two months before Apple introduced the first iPhone. See Ritchie, History of iPhone: Apple Reinvents the Phone, iMore (Aug. 22, 2014), at [www.imore.com/history-iphone-2g](http://www.imore.com/history-iphone-2g) (last viewed Mar. 27, 2015) (detailing the history of

the iPhone and its launch date of June 29, 2007). Although the use of simpler, less powerful cell phones was well established by then, neither the Court nor the litigants could have been expected to predict the life-changing smartphone revolution about to begin. Accordingly, McDermott's statement that "[a]dvance approval for the particular methods to be used in the forensic examination of the computers and disks is not necessary," 448 Mass. at 776, bears reassessment. In more recent cases involving the searches of computers, courts -- including this one -- have acknowledged the need to segregate, using third party engineers if necessary, the particular files for which the government has established probable cause from those for which it has not and which it therefore cannot have lawful authority to search. See Preventive Med. Associates, Inc. v. Commonwealth, 465 Mass. 810, 830-832 (2013) (distinguishing McDermott and stating: "We take seriously the concern that a cursory review of every e-mail undermines the particularity requirement [because such a review may] enable the Commonwealth to use against the defendants inculpatory evidence with respect to the pending indictments that it finds in the emails, even though such evidence may not actually

fit within the scope of the search warrants obtained." ). See also United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1170-1172 (9th Cir. 2010) (finding that examination of data for which government did not have probable cause was "an obvious case of deliberate overreaching by the government"); id. at 1180 (Kozinski, C.J., concurring) ("The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents." ).

Smartphones are so powerful and so widespread throughout society that the risk of overreach by the police has grown exponentially since 2007. The magistrate who reviewed the Dorelas warrant application may well have had McDermott's statement in mind. At the same time, the magistrate may not have realized that police possessed a device -- the UFED -- that allowed them easily and conveniently to limit the smartphone files for which probable cause existed. A description in a warrant application explaining how a data extraction will occur and how the device performing the extraction can or cannot be used to



limit the scope of the search is not too onerous a burden to impose.

**D. Smartphones Also Deserve Heightened Protection Because They Contain Constitutionally Protected Speech and Associational Information.**

In addition to containing large amounts of data revealing the most private aspects of a person's life, smartphones also contain expressive and associational materials. Warrant applications seeking authority to search and seize books, documents, photographs, videos and other expressive material, merit extra care and attention from the reviewing magistrate, and extra caution and restraint by the police.

What the history of search and seizure jurisprudence "indispensably teaches is that the constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain." Stanford v. Texas, 379 U.S. 476, 485 (1965). In that case, the Court found a warrant authorizing the search and seizure of "literary material[,] 'books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments" to be of

"indiscriminate sweep" and "constitutionally intolerable." Id. at 486. See also Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978) ("Where presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field."); Commonwealth v. Dane Entertainment Services, Inc., 389 Mass. 902, 906 (1983) ("Because of the possibility of interference with protected materials, police seizure of allegedly obscene books and films 'calls for a higher hurdle in the evaluation of reasonableness.' Thus, before police obtain a warrant to seize a film, a magistrate must have an opportunity 'to focus searchingly on the question of obscenity.'" [citations omitted])).

Photographs, like books and essays, can be protected forms of expression. "Visual art is as wide ranging in its depiction of ideas, concepts and emotions as any book, treatise, pamphlet or other writing, and is similarly entitled to full First Amendment protection." Bery v. City of New York, 97 F.3d 689, 695 (2d Cir. 1996). While every form of photography is not eligible for such protection, see Larsen v. Fort Wayne Police Dept., 825 F. Supp. 2d

965, 979-980 (N.D. Ind. 2010) (videotape for documentation of daughter's childhood not protected), the police should not be allowed to indiscriminately examine a smartphone file that may contain thousands of photographs without undergoing some form of heightened scrutiny. At a minimum, a magistrate should require the police to demonstrate that there is little to no probability that they are invading a form of protected expression.

The search of a smartphone also triggers a risk that protected associational activity will be invaded. While initially regarded as a device for connecting with friends and relatives, smartphones have increasingly become a tool used for political activity and other forms of community involvement. Smartphones now contain a broad range of social networking applications, and those applications have become a pervasive means of sending and receiving information about political campaigns, fundraising, and other forms of collective activity. The search of a smartphone increasingly presents a risk of revealing associational information that courts have traditionally forbidden the government from compelling

a person to divulge absent extraordinary circumstances.

The First Amendment protects a person from the compelled disclosure of his or her group memberships and other associations. See NAACP v. Alabama, 357 U.S. 449, 460 (1958). Privacy in group association is often indispensable to the preservation of freedom of association -- especially when unpopular or dissident beliefs are concerned. Absent that degree of privacy, individuals would feel pressured to "adhere to the most orthodox and uncontroversial view and associations." Watkins v. United States, 354 U.S. 178, 197-198 (1957). Forced disclosure harms both the person forced to disclose and those with whom he or she chose to associate. Id. at 197.

Smartphones contain substantial quantities of information about our associations, and internet-enabled smartphones have accelerated the development of associational features. Social networking applications have become an important means of promoting a person's views, of petitioning, and of other forms of political activity. For Americans who use their smartphones to associate with particular candidates and campaigns, a police search of these

phones presents a substantial risk of law enforcement uncovering information about the phone owner's political associations and beliefs. The risk of invading these rights requires magistrates to give smartphone search warrant applications an exacting scrutiny that demands strict compliance with the twin mandates of probable cause and particularity.

#### V. CONCLUSION

Amicus Curiae, the American Civil Liberties Union of Massachusetts, respectfully urges this Court to reverse the decision below. A reversal will send an unmistakable message about the importance of adhering to the constitutional principles of probable cause and particularity in the digital age.

Respectfully submitted,

**AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MASSACHUSETTS**

*Robert E. McDonnell* *ALC*

Robert E. McDonnell

BBO #331470

robert.mcdonnell@morganlewis.com

John Frank Weaver

BBO #673374

john.weaver@morganlewis.com

Arcangelo S. Cella

arcangelo.cella@morganlewis.com

**MORGAN, LEWIS & BOCKIUS LLP**

One Federal Street

Boston, MA 02110-1726

617.341.7700

Matthew R. Segal, BBO #654489

MSegal@aclum.org

Jessie J. Rossman, BBO #670685

JRossman@aclum.org

Mason Kortz, BBO #691257

MKortz@aclum.org

The American Civil Liberties

Foundation of Massachusetts

211 Congress Street

Boston, MA 02110

617.482.3170

Dated: March 27, 2015

CERTIFICATION PURSUANT TO  
MASSACHUSETTS RULE OF APPELLATE PROCEDURE 16

I hereby certify that, to the best of my knowledge, the brief filed herewith complies with the Massachusetts Rules of Appellate Procedure that pertain to the filing of briefs, including, without limitation, Rule 16 and Rule 20.



Robert E. McDonnell

BBO #331470

robert.mcdonnell@morganlewis.com

**MORGAN, LEWIS & BOCKIUS LLP**

One Federal Street

Boston, MA 02110-1726

617.341.7700

COMMONWEALTH OF MASSACHUSETTS

SUPREME JUDICIAL COURT

---

No. SJC-11793

---

COMMONWEALTH OF MASSACHUSETTS

Appellee

v.

DENIS DORELAS

Defendant-Appellant

---

**CERTIFICATE OF SERVICE**

---

I, Robert E. McDonnell, hereby certify that  
on March 27, 2015, I served the attached Brief of  
*Amicus Curiae* Massachusetts Civil Liberties Union, by  
mailing copies thereof, postage prepaid, to:

Nancy Dolberg, Esq.  
Committee for Public  
Counsel Services  
Public Defender Division  
44 Bromfield Street  
Boston, MA 02108  
Phone: 617-482-6212  
ndolberg@publiccounsel.net

John P. Zanini, Esq.  
Office of the District  
Attorney for Suffolk  
County  
One Bullfinch Place  
Boston, MA 02114  
Phone: 617-619-4070  
Jack.Zanini@state.ma.us



Robert E. McDonnell  
BBO #331470  
robert.mcdonnell@morganlewis.com  
**MORGAN, LEWIS & BOCKIUS LLP**  
One Federal Street  
Boston, MA 02110-1726  
617.341.7700



## **ADDENDUM**

### **First Amendment to the Constitution of the United States**

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

### **Fourth Amendment to the Constitution of the United States**

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.

### **Article 14 of the Massachusetts Declaration of Rights**

Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.

### **G.L. c. 265, § 15. Assault; intent to murder or maim; penalty**

Whoever assaults another with intent to commit murder, or to maim or disfigure his person in any way described in the preceding section, shall be punished

by imprisonment in the state prison for not more than ten years or by a fine of not more than one thousand dollars and imprisonment in jail for not more than two and one half years.

**G.L. c. 265, § 15B. Assault with dangerous weapon; victim sixty or older; punishment; subsequent offenses**

(a) Whoever, by means of a dangerous weapon, commits an assault upon a person sixty years or older, shall be punished by imprisonment in the state prison for not more than five years or by a fine of not more than one thousand dollars or imprisonment in jail for not more than two and one-half years.

Whoever, after having been convicted of the crime of assault upon a person sixty years or older, by means of a dangerous weapon, commits a second or subsequent such crime, shall be punished by imprisonment for not less than two years. Said sentence shall not be reduced until one year of said sentence has been served nor shall the person convicted be eligible for probation, parole, furlough, work release or receive any deduction from his sentence for good conduct until he shall have served one year of such sentence; provided, however, that the commissioner of correction may, on the recommendation of the warden, superintendent, or other person in charge of a correctional institution, or the administrator of a county correctional institution, grant to said offender a temporary release in the custody of an officer of such institution for the following purposes only: to attend the funeral of next of kin or spouse; to visit a critically ill close relative or spouse; or to obtain emergency medical services unavailable at said institution. The provisions of section eighty-seven of chapter two hundred and seventy-six relative to the power of the court to place certain offenders on probation shall not apply to any person 18 years of age or over charged with a violation of this subsection.


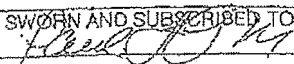
For the purposes of prosecution, a conviction obtained under subsection (a) of section fifteen A or paragraph (a) of section 18 shall count as a prior criminal conviction for the purpose of prosecution and sentencing as a second or subsequent conviction.

(b) Whoever, by means of a dangerous weapon, commits an assault upon another shall be punished by imprisonment in the state prison for not more than five years or by a fine of not more than one thousand dollars or imprisonment in jail for not more than two and one-half years.

# APPENDIX

## APPENDIX

	Page
Application for Search Warrant.....	A. 1
Affidavit in Support of Application for Search Warrant .....	A. 3
Search Warrant.....	A. 6
Return of Officer Serving Search Warrant .....	A. 8
Memorandum of Decision and Order on Motions to Suppress Statements.....	A. 10
Memorandum and Order on Defendant's Motions to Suppress Evidence.....	A. 14
Universal Forensic Extraction Device (UFED) User Manual .....	A. 19

APPLICATION FOR SEARCH WARRANT G.L.c. 276, §§ 1-7		TRIAL COURT OF MASSACHUSETTS Criminal COURT DEPARTMENT	
NAME OF APPLICANT Richard Walker		West Roxbury DIVISION	
POSITION OF APPLICANT Boston Police Detective		SEARCH WARRANT DOCKET NUMBER 1106 SW 089	
I, the undersigned APPLICANT, being duly sworn, depose and say that:			
1. I have the following information based upon the attached affidavit(s), consisting of a total of 03 page(s), which is (are) incorporated herein by reference.			
2. Based upon this information, there is PROBABLE CAUSE to believe that the property described below:			
<input type="checkbox"/> has been stolen, embezzled, or obtained by false pretenses <input type="checkbox"/> is intended for use or has been used as a means of committing a crime. <input type="checkbox"/> has been concealed to prevent a crime from being discovered. <input type="checkbox"/> is unlawfully possessed or concealed for an unlawful purpose. <input checked="" type="checkbox"/> is evidence of a crime or is evidence of criminal activity. <input type="checkbox"/> other (specify) _____			
3. I am seeking the issuance of a warrant to search for the following property (describe the property to be searched for as particularly as possible): <u>Apple I phone, silver &amp; black. Green soft case recovered pursuant to 1106 SW 089 to retrieve</u>			
Subscriber's name and telephone number, contact list, address book, calendar, date book entries, group list, speed dial list, phone configuration information and settings, incoming and outgoing draft sent and deleted text messages, saved opened, unopened draft sent and deleted electronic mail messages, mobile instant message chat logs and contact information mobile internet browser and saved and deleted photographs which are on an Apple iPhone silver and black, cracked screen in a green soft rubber case. Additionally information from the networks and carriers such as subscriber's information, call history containing use times and number dialed, called, received and missed.			
4. Based upon this information, there is also probable cause to believe that the property may be found (check as many as apply):			
<input checked="" type="checkbox"/> at (identify the exact location or description of the place(s) to be searched): Custody of Boston Police Department, 1249 Hyde Park Ave., Hyde Park, Ma.			
which is occupied by and/or in the possession of: Boston Police Department			
<input type="checkbox"/> on the person or in the possession of (identify any specific person(s) to be searched):			
<input type="checkbox"/> on any person present who may be found to have such property in his or her possession or under his or her control or to whom property may have been delivered.			
THEREFORE, I respectfully request that the court issue a Warrant and order of seizure, authorizing the search of the above described place(s) and person(s), if any, to be searched, and directing that such property or evidence or any part thereof, if found, be seized and brought before the court, together with such other and further relief that the court may deem proper.			
<input type="checkbox"/> have previously submitted the same application. <input checked="" type="checkbox"/> have not previously submitted the same application.			
PRINTED NAME OF APPLICANT Richard Walker		SIGNED UNDER THE PENALTIES OF PERJURY  Signature of Affiant	
SWORN AND SUBSCRIBED TO BEFORE 		9-15-11	

RA 11

Signature of Justice, Clerk-Magistrate or Assistant Clerk	Date	9-15-11	etc
110630089			

RA 12

1106 SW 089

etc

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT	TRIAL COURT OF MASSACHUSETTS
--	---------------------------------

1. I, Richard Walker, am a Boston Police Officer and have been a police officer for 26 year(s). I am presently assigned to Boston Police Area E-18 Detectives Unit as a criminal investigator and have been so assigned for the last 11 year(s). During that time I have investigated and processed numerous serious and violent crimes, including assault and battery dangerous weapon, and have received specialized training and experience in the collection of physical evidence, crime scene processing, and the investigations of such cases. I have personal knowledge of the facts and circumstances hereinafter related as a result of my own investigative efforts and those of brother officers, who have reported their findings to me.

2. Based upon my personal knowledge, I believe that the crime of Assault and Battery with a Dangerous Weapon to wit a Firearm, a violation of Massachusetts General Laws, Chapter 265, Section 15B, Assault with Intent to Murder, a violation of Massachusetts General Laws, Chapter 265, Section 15, was committed at 74 Pierce Street, Hyde Park, Massachusetts and the victims/suspects being identified as one Michael Lerouge and Denis Junior Keri Dorelas in that the facts establishing the grounds for my request to the court for the issuance of a search warrant are as follows:

3. On 07/03/2011, about 7:08 P.M., I responded with other Area E-18 Detectives, Detective Supervisors, and Police Officers, to 74 Pierce Street, Hyde Park, for a radio call of a person shot. On arrival responding unit found a Michael Lerouge suffering from a gunshot wounds to back area. Mr. Lerouge was transported to the Brigham and Women's Hospital by Emergency Medical Technicians for treatment. Denis Junior Keri Dorelas was located on a concrete landing on the left side of 86 Pierce Street, suffering from gunshot wounds to his left legs. Mr. Dorelas was transported to Beth Israel Hospital by EMT's for further treatment.

4. On arrival at 74 Pierce Street, Officer Boyle located a black firearm in the middle of the roadway between 73 and 74 Pierce Street. This black firearm is a Glock 23, .40 caliber with serial number KDT930. This firearm was in the locked back position indicating that the firearm was fired until the magazine was empty. The firearm contained an empty magazine that had the capacity to store 13 rounds of ammunition. Due to growing number of onlookers and for safety concerns, Officer Boyle retrieved this firearm which was turned over to Officer Rogers who handed said firearm to Detective Walker. Witnesses who are known to the Commonwealth of Massachusetts stated that the shooting victim identified as Michael Lerouge discarded the black Glock 23 under a parked m/v. Firearm failed to stop under the parked m/v and slid into the street where it was recovered by Officer Boyle.

5. Witnesses on scene informed the responding officers that two black males were shooting at each other in the vicinity of 74 Pierce Street. The witnesses who are known to the Commonwealth stated that Mr. Lerouge was one of the shooters. They stated that the other shooter ran on Pierce Street towards Walter Street. The witnesses stated that this black male dropped a firearm as he ran. He stopped, retrieved the firearm and ran to 86 Pierce Street. This male was described as wearing a green colored shirt/jacket with some type of writing on it. Denis Junior Keri Dorelas was located on the left side of 86 Pierce Street suffering from gunshot wounds to his left leg. Mr. Dorelas was wearing a green colored jacket with emblems on it. Mr. Dorelas was in the company of Jamal Boucicault.

6. Jamal Boucicault was transported to Area E-18 where he was interviewed by Detectives Antonucci and Morris. Mr. Boucicault was informed of his right to have the interview electronically recorded and declined to have the interview electronically recorded. During the interview Mr. Boucicault stated that he was visiting his friend, Denis Junior Keri Dorelas, at 86 Pierce Street, second floor rear apartment (a converted porch). Mr. Boucicault stated that Mr. Dorelas received a phone call and started arguing with the caller on the phone. Mr. Boucicault stated that Mr. Dorelas left the apartment still arguing with the caller. Mr. Boucicault stated that he remained in the apartment playing games on a laptop. Mr. Boucicault stated that a short time after Mr. Dorelas

RA 12



1106SW089

left the apartment he heard what sounded like gunshots. Mr. Boucicault stated that he ventured outside where he observed Mr. Dorelas on a concrete landing on the left side of the house at 86 Pierce Street. Mr. Boucicault stated that he was given a gun by Mr. Dorelas and was instructed by Mr. Dorelas to hide the gun. Mr. Boucicault stated that he took the gun upstairs to the second floor rear apartment which belongs to Mr. Dorelas and hid the gun behind either a washing machine or a clothes dryer in Mr. Dorelas' apartment.

7. While on scene Detective Walker interviewed Bricknell Dorelas who stated he is the brother of Denis Junior Keri Dorelas. Bricknell Dorelas stated that earlier in the evening he received a telephone call from Denis Junior Keri Dorelas. Bricknell stated that his brother informed him that he was receiving threatening phone calls and threatening text messages on his phone. Bricknell stated that he came to 86 Pierce Street and visited his brother who he encouraged to stay in the house and not to get entangled with the caller who was threatening him. Bricknell stated that he doesn't know the identity of the person who is threatening his brother. Detective Walker also interviewed Mr. Jean Vincent who stated that he is the owner of 86 Pierce Street, Hyde Park, Massachusetts. Mr. Vincent stated that he rent the rear apartment on the second floor of 86 Pierce Street to Mr. Denis Junior Keri Dorelas. Mr. Vincent stated that Mr. Dorelas have been living at 86 Pierce Street, Hyde Park, since March 2011, and is the sole occupant of this apartment.

8. While on scene Sgt. Det. Casinelli interviewed Ohuinel Normil who is the cousin of Denis Junior Keri Dorelas. Ohuinel Normil stated that Denis has been getting a lot of telephone threats because he owes money to people. Mr. Normil stated that he doesn't know the identity of the people who are threatening Mr. Dorelas.

9. Blood stained clothing from both Mr. Dorelas and Mr. Lerouge were seized at the scene and is being held as evidence to be further examined by Boston Police Crime Lab pending the issuance of a search warrant. Additional clothing from Mr. Lerouge was seized at Brigham and Womens Hospital and will be held and examined By Boston Police Crime Lab pending the issuance of a search warrant. Additional clothing from Mr. Dorelas was seized at Beth Israel Hospital and will be held to be examined by Boston Police Crime Lab pending the issuance of a search warrant.

10. On 07/04/2011, about 5:58 P.M., West Roxbury District Court Search Warrant 1106SW065, was executed at 86 Pierce Street, Hyde Park, second floor rear apartment. Pursuant to the search warrant on Apple iPhone, silver and black with a green soft rubber cover and a cracked screen was seized. During a conversation with Officer Cox, said cell phone was described to Mr. Dorelas and he stated that the cell phone belonged to him.

11. Based on the above facts of Mr. Dorelas stating that he had telephone conversation with his attacker prior to being attacked and both Bricknell Dorelas and Ohuinel Normil stating that Mr. Dorelas has been receiving telephone threats via his cell phone I have probable cause to believe Mr. Dorelas cell phone contains valuable information that will link the victim/suspect (Dorelas) and suspect/victim (Lerouge) to the crime.

12. Based upon the foregoing facts and information, I am seeking the Honorable Court's permission to search the Apple iPhone, silver and black, green soft rubber cover and cracked screen. Electronic Device information from the cellular phone such as phone numbers and direct connect numbers in the address book, phone numbers and call history, direct connect numbers called, received calls, missed calls, text messages, e-mails, instant messages, videos, pictures and picture messages. Additionally, information from the network and carrier such as subscriber's information, call history containing use times and numbers dialed, called received and missed.

- A. Subscriber telephone number.
- B. Electronic Serial Number, International Mobile Equipment Identity, Mobile Equipment Identifier, or similar identification number.
- C. Contact list, address book, calendar, and date-book entries.
- D. Group list.
- E. Speed dial list.
- F. Phone configuration information and settings.

RA 14

( 110656087

- G. Incoming, outgoing, draft sent and deleted text messages.  
 H. Saved, opened, and unopened voice mail messages.  
 I. Saved, opened, unopened, draft, sent and deleted electronic mail messages.  
 J. Mobile instant message and logs, data, and contact information.  
 K. Mobile Internet browser history.  
 L. Saved and deleted photographs and movies.

PRINTED NAME OF AFFIANT	SIGNED UNDER THE PENALTIES OF PERJURY
Richard Walker	<i>[Signature]</i> Signature of Affiant
SWORN AND SUBSCRIBED TO BEFORE	9-15-11
<i>[Signature]</i> Signature of Justice, Clerk-Magistrate or Assistant Clerk	Date

RA 15

SEARCH WARRANT		TRIAL COURT OF MASSACHUSETTS	
G.L.c. 276, §§ 1-7		Criminal	COURT DEPARTMENT
NAME OF APPLICANT		West Roxbury	DIVISION
Richard Walker		SEARCH WARRANT DOCKET NUMBER	
POSITION OF APPLICANT		1109 SW 089	
Boston Police Detective			
TO THE SHERIFFS OF OUR SEVERAL COUNTIES OR THEIR DEPUTIES, ANY STATE POLICE OFFICER, OR ANY CONSTABLE OR POLICE OFFICER OF ANY CITY OR TOWN, WITHIN OUR COMMONWEALTH:			
Proof by affidavit, which is hereby incorporated by reference, has been made this day and I find that there is PROBABLE CAUSE to believe that the property described below			
<input type="checkbox"/> has been stolen, embezzled, or obtained by false pretenses <input type="checkbox"/> is intended for use or has been used as a means of committing a crime. <input type="checkbox"/> has been concealed to prevent a crime from being discovered. <input type="checkbox"/> is unlawfully possessed or concealed for an unlawful purpose. <input checked="" type="checkbox"/> is evidence of a crime or is evidence of criminal activity. <input type="checkbox"/> other (specify) _____			
YOU ARE THEREFORE COMMANDED within a reasonable time and in no event later than seven days from the issuance of this search warrant to search for the following property: <u>Apple I Phone Silver &amp; Black Green Soft Rubber Case</u> Subscriber's name and telephone number, contact list, address book, calendar, date book entries, group list, speed dial list, phone configuration information and settings, incoming and outgoing draft sent, deleted text messages, saved, opened, unopened draft sent and deleted electronic mail messages, mobile instant message chat logs and contact information mobile internet browser and saved and deleted photographs on an Apple iPhone, silver and black, green soft rubber case. Additionally, information from the networks and carriers such as subscribers information, call history information, call history containing use times and numbers dialed, called, received and missed.			
<input type="checkbox"/> at: Boston Police Department, 1249 Hyde Park Ave., Hyde Park, Ma.			
which is occupied by and/or in the possession of: Boston Police Department			
<input type="checkbox"/> on the person or in the possession of:			
You <input type="checkbox"/> are <input checked="" type="checkbox"/> are not also authorized to conduct the search at any time during the night.			
You <input type="checkbox"/> are <input checked="" type="checkbox"/> are not also authorized to enter the premises without announcement.			
You <input type="checkbox"/> are <input checked="" type="checkbox"/> are not also commanded to search any person present who may be found to have such property in his or her possession or under his or her control or to whom such property may have been delivered.			
YOU ARE FURTHER COMMANDED if you find such property or any part thereof, to bring it, and when appropriate, the persons in whose possession it is found before the West Roxbury Division of the Criminal Court Department.			

COPIED PURSUANT TO 1106B-W 065 TO RETAIN

RA 16

DATE ISSUED 9-15-11	SIGNATURE OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK <i>Paul F. Tagli</i>
FIRST OR ADMINISTRATIVE JUSTICE	PRINTED NAME OF JUSTICE, CLERK-MAGISTRATE OR ASSISTANT CLERK
WITNESS: KATHLEEN CERRY	PAUL F. TAGLI

RETURN OF OFFICER SERVING SEARCH WARRANT

*A search warrant must be executed as soon as reasonably possible after its issuance, and in any case may not be validly executed more than 7 days after its issuance. The executing officer must file his or her return with the court named in the warrant within 7 days after the warrant is issued. G.L.c. 276, §3A.*

This search warrant was issued on September 15<sup>th</sup>, 2011, 2007, and I have executed it as follows:

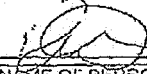
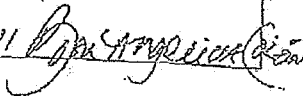
The following is an inventory of the property taken pursuant to this search warrant:

1. Phone Examination Report Properties
2. Phone Examination Report Index
3. Phone Contacts
4. Phone Incoming Call List
5. Phone Outgoing Call List
6. Phone Missed Call List
7. Images
8. Video
9. \_\_\_\_\_
10. \_\_\_\_\_
11. \_\_\_\_\_
12. \_\_\_\_\_
13. \_\_\_\_\_
14. \_\_\_\_\_
15. \_\_\_\_\_
16. \_\_\_\_\_
17. \_\_\_\_\_
18. \_\_\_\_\_
19. \_\_\_\_\_
20. \_\_\_\_\_
21. \_\_\_\_\_
22. \_\_\_\_\_
23. \_\_\_\_\_
24. \_\_\_\_\_
25. \_\_\_\_\_
26. \_\_\_\_\_

This inventory was made in the presence of: Det. Kevin Witherspoon

I swear that this inventory is a true and detailed account of all the property taken by me  
on this search warrant

RA 18

SIGNATURE OF PERSON MAKING SEARCH X 	DATE AND TIME OF SEARCH 09/15/2011 6:17 P.M.	SWORN AND SUBSCRIBED TO BEFORE X 9/21/2011
PRINTED NAME OF PERSON MAKING SEARCH Richard Walker	TITLE OF PERSON MAKING SEARCH Detective	DATE SWORN AND SUBSCRIBED TO 9-21-2011 

RA 19

16

Suffolk, ss. Commonwealth of Massachusetts Ind. 11-10948  
Superior Court

COMMONWEALTH

v.

DENIS DORELAS

MEMORANDUM OF DECISION AND ORDER  
ON MOTIONS TO SUPPRESS STATEMENTS

A. Introduction

The defendant is charged with unlawful possession of a firearm, ammunition, a loaded firearm and a large capacity ammunition feeding device. The defendant's two motions to suppress seek suppression of statements the defendant made to a police officer while he was being treated for gunshot injuries in a hospital. The defendant's statements must be suppressed under the exclusionary rule established by the Supreme Judicial Court in *Commonwealth v. Rosario*, 422 Mass. 48, 56-57 (1996).

B. The July 6 Hospital Statements

On the evening of July 3, 2011, Boston Police officers and EMT's responded to reports of a shooting incident on Pierce Street in Hyde Park. The defendant had sustained multiple gunshot wounds in his left leg. Michael Larouge was also shot in the same incident.

Detective Richard Walker spoke to the defendant briefly as he was about to be put on a stretcher. The defendant said that he got shot and that he was in a lot of pain. The defendant was taken to Beth Israel Deaconess Medical Center and admitted. Michael Larouge was taken to a separate hospital.

A bullet or bullets had broken the defendant's left femur. The defendant was treated at the Beth Israel Deaconess hospital until July 8.

The investigating officers had information that the defendant and Mr. Larouge had fired shots at each other causing gunshot injuries to both men. At some point on July 3, after the defendant's arrival at the hospital, officers placed the defendant under arrest. Officers also arrested Mr. Larouge. The preliminary charges against the defendant included armed assault with intent to murder and unlawful possession of a firearm and ammunition. The defendant was handcuffed by one hand to his hospital bed. He was guarded by one or two Boston Police officers around the clock.

On July 4, the defendant had a major surgical procedure with irrigation, debridement and an open reduction with internal fixation on his broken femur. The defendant was regularly receiving narcotic pain medications between at least July 4 and his hospital discharge. He was discharged from the hospital on July 8. He was taken in police custody to the West Roxbury Division of the Boston Municipal Court. The defendant was arraigned in that court on July 8.

On Wednesday, July 6, Boston Police Officer Edward Cox guarded the defendant at the hospital on an overtime assignment from 4:00 p.m. on July 6 until 1:00 a.m. on July 7. Officer Cox had not been involved in any part of the police response to the shooting and gun possession incident. Although he had a basic idea of what the defendant's charges were, Officer Cox did not

know how or why the defendant had been arrested. Officer Cox did not have any prior knowledge about the defendant.

The defendant initiated a conversation with Officer Cox during the night hours prior to midnight on the night of July 6. The defendant was curious about what would happen to him with his charges. He tried to probe Officer Cox about this. Officer Cox acted in a friendly, conversational manner with the defendant. He did not initiate the conversation relating to the defendant's shooting and gun possession incident. The defendant told Officer Cox that another man had shot him. The defendant said that he went to the ground when he was hit. He said that when he was on the ground he took out a gun and shot back at the other man. He said that the other man's name was Larouge. The defendant may have added some other information about the shooting or his gun possession.

At some point in their July 6 conversation, Officer Cox asked some questions about the incident as a natural follow-up part of a two-way conversation with the defendant. In his testimony, Officer Cox could not clearly remember whether and when he asked any questions in this conversation. This is not surprising considering the fifteen months that passed between the conversation and his testimony at the motion hearing. Officer Cox was genuinely interested in the defendant's personal welfare. He wanted to help him avoid getting shot, avoid criminal activity and avoid people who would be likely to lead him into criminal activity. It was the defendant who began the conversation by trying to find out from Officer Cox what would happen with his charges. Nevertheless, the court is unable to find that the defendant's statements about the shooting and gun possession incident were not made in response to questions from Officer Cox. Once the defendant started talking about the incident, Officer Cox's follow-up questions were reasonably likely to result in incriminating answers from the defendant.

The Miranda warnings and waiver requirements do not apply unless a defendant's statement is in response to custodial interrogation. *Rhode Island v. Innis*, 446 U.S. 291, 300-01 (1980). Interrogation includes both "express questioning" and "any words or actions on the part of the police (other than those normally attendant to arrest and custody) that the police should know are reasonably likely to elicit an incriminating response from the suspect." *Id.*; *Arizona v. Mauro*, 481 U.S. 520, 526-527 (1987); *Commonwealth v. Torres*, 424 Mass. 792, 796-798 (1997). As the Court stated in *Miranda* "[v]olunteered statements of any kind are not barred by the Fifth Amendment and their admissibility is not affected by our holding today." *Miranda v. Arizona*, 384 U.S. 436, 478 (1966).

The defendant's July 6 statements about the facts of the shooting and gun possession are not admissible because there were no Miranda warnings and because the court is unable to find from the evidence that the defendant's statements were not in response to some questions by Officer Cox that were reasonably likely to elicit an incriminating response, even though that was not the officers' intent.

With respect to the Supreme Judicial Court's *Rosario* rule, this rule prohibits "police questioning of an arrested person" more than six hours after the arrest unless the defendant has made an informed and voluntary written or recorded waiver of his right to be arraigned without unreasonable delay. *Commonwealth v. Rosario*, 422 Mass. 48, 56-57 (1996). In applying the *Rosario* rule to police questioning, the court will use the *Rhode Island v. Innis* definition of interrogation.



It is difficult to determine when the six-hour *Rosario* period began to run. The defendant was admitted to the hospital on July 3. He underwent major surgery on July 4. He could not properly be interrogated on those days due to his medical disability. See *Rosario*, 422 Mass. at 56-57; *Commonwealth v. Tran*, 460 Mass. 535, 562 (2011) (exceptional circumstances may permit a delay in the start of the six-hour period). The precise time when the disability ended is unknown. The court finds, however, that by the afternoon of July 6, two days after the surgery, the defendant had recovered sufficiently so that he could voluntarily and competently participate in police questioning about the shooting and gun possession incident. Officer Cox's July 6 conversation with the defendant occurred in the night hours before midnight. The court finds that this conversation about the shooting and gun possession incident occurred more than six hours after the defendant was no longer incapacitated for purposes of police questioning. There was no written or recorded waiver of the right to a prompt arraignment. The statements are not admissible under the *Rosario* rule.

#### C. The July 7 Hospital Statements

Boston Police Detective Richard Walker went to the hospital on July 4 or 5 to interview the defendant about the shooting and gun possession incident. He learned that the defendant's medical condition was not good enough for a police interview. Detective Walker returned to the hospital on July 7 at about 9:00 a.m. with a second detective. The defendant's medical condition at that time was good enough for a police interview. The detectives gave the defendant Miranda warnings. The defendant said he wanted a lawyer. The detectives ended the interview attempt.

Officer Cox was again assigned to guard the defendant beginning at 4:00 p.m. on July 7. This overtime assignment was based on ordinary overtime procedures; it had nothing to do with the investigation of the charges against the defendant.

Before speaking with the defendant on July 7, Officer Cox had spoken with Detective Walker and Lieutenant Cruz about his conversation with the defendant on July 6. Detective Walker told Officer Cox that he had tried to interview the defendant on the morning of July 7. He told him that the officers terminated the interview because the defendant had asked to speak with a lawyer. Detective Walker or Lieutenant Cruz told Officer Cox that if the defendant initiated a conversation about the incident Officer Cox should give him Miranda warnings and let him say what he wanted to say.

On the night of July 7, the defendant initiated a conversation with Officer Cox about the shooting and gun possession incident. Officer Cox told the defendant that he had invoked the right to counsel and that he could not speak with him about the incident unless he revoked his counsel request and waived the right to counsel. The defendant said that he wanted to speak to Officer Cox and waive his right to counsel. Officer Cox read the defendant Miranda warnings from a card. The defendant and Officer Cox then discussed the incident. The defendant told Officer Cox some details about his shooting incident with Michael Larouge. The defendant told the officer about how he acquired the gun that he used. He also gave information about Michael Larouge and some other persons that the defendant knew in Hyde Park.

Officer Cox's July 7 conversation with the defendant about the incident did not comply with the *Rosario* requirements. The *Rosario* case has created a per se rule of exclusion, even if the defendant's initiation of the discussion and his *Miranda* rights were sufficient under the

requirements of *Edwards v. Arizona*, 451 U.S. 477, 484-485 (1981). Although the conversation was initiated by the defendant, the court finds that the conversation included questions and conversation by Officer Cox that were reasonably likely to elicit an incriminating response. The court is unable to find from the evidence any particular statement by the defendant that was not part of the back-and-forth mutual discussion with Officer Cox, including questions by the officer.


By the night of July 7, the defendant had been medically competent to participate in a police interview for over six hours. There was no written or recorded waiver of the right to a prompt arraignment. The defendant's July 7 statements must be suppressed under the Supreme Judicial Court's *Rosario* decision.

The defendant's medical condition on July 6 and 7 was not suitable for taking him to court for an arraignment. Although arraignments are sometimes conducted in hospitals, neither the court nor the police were required to arrange a hospital arraignment. The delay in the arraignment in this case was not caused by the police. Nevertheless, the *Rosario* rule requires that there must be a written or recorded waiver of the right to a prompt arraignment if the questioning occurs more than six hours after the defendant is no longer incapacitated for an interview.<sup>1</sup>

D. Order

The defendant's statements to Officer Cox while he was in the hospital are suppressed.

November 7, 2012

  
Charles J. Hely  
Justice

---

<sup>1</sup>Because the *Rosario* rule requires suppression of the July 7 statements, the court need not determine whether the July 7 statements were based on "a voluntary, knowing, and intelligent waiver of the right to have counsel present and of the right to remain silent" despite the July 6 Miranda violation. *Commonwealth v. Rankins*, 429 Mass. 470, 473 (1999); *Commonwealth v. Torres*, 424 Mass. 792, 799 (1997).

3/14/2013 filed

24

SUFFOLK, SS

COMMONWEALTH OF MASSACHUSETTS

SUPERIOR COURT  
NO. 11-10948

COMMONWEALTH

v.

DENNIS DORELAS, DEFENDANT

MEMORANDUM AND ORDER ON DEFENDANT'S MOTIONS TO SUPPRESS  
EVIDENCE

The defendant, charged with possession of a firearm and related offenses, has filed two late motions to suppress. The first motion to suppress, filed on February 28, 2013, seeks to suppress any "evidence obtained as a result of an electronic search of a cell phone seized from 86 Pierce Street in Roslindale." The cell phone itself, the physical object, was seized pursuant to a search warrant. Data from the cell phone, including photographs of the defendant in a green jacket<sup>1</sup> and with a gun, was seized pursuant to a separate search warrant issued on September 15, 2011. The second motion to suppress, filed on March 4, 2013, seeks to suppress the photographs and a video seized after the electronic search of the cell phone following the second warrant.

Defendant's argument on his first motion is that any references in the officer's affidavit to statements made by him to the police must not be considered in determining probable cause because those statements were suppressed by Judge Hely due to a Rosario violation on November 7, 2012. The defendant is correct that the defendant's statements which were

---

<sup>1</sup> A witness told the police that one of the men involved in the shooting was wearing a green jacket.

suppressed must not be considered in evaluating probable cause for the warrant. The officer's affidavit, however, otherwise contains sufficient information for the magistrate to conclude that defendant was the sole occupant of the apartment at 86 Pierce Street, and that the defendant was the recent recipient of threatening telephone calls and messages. Defendant's sole occupancy of the apartment makes it probable that any cell phones therein belonged to him. The affidavit did not have to eliminate all speculative possibility that cell phones found in the apartment may have belonged to others.

The search warrant of September 15, 2011 describes the property to be searched as:

Apple iPhone silver and black green soft case recovered pursuant to 1106SW065 to retrieve subscriber's name and telephone number, contact list, address book, calendar, date book entries, group list, speed dial list, phone configuration information and settings, incoming and outgoing draft sent, deleted text messages, saved, opened, unopened draft sent and deleted electronic mail messages, mobile instant message chat logs and contact information mobile Internet browser and saved and deleted photographs on an Apple iPhone, silver and black, green and soft rubber case. Additionally, information from the networks and carriers such as subscribers information, call history information, call history containing use times and numbers dialed, called, received and missed.

The inventory return lists the following taken as result of the search warrant:

1. Phone Examination Report Properties
2. Phone Examination Report Index
3. Phone Contacts
4. Phone Incoming Call List
5. Phone Outgoing Call List
6. Phone Missed Call List
7. Images
8. Video

The defendant's motion seeks to suppress all "photographs and videos" seized.

Photographs are covered by the search warrant; videos do not appear to be.

Of course search warrants must be particularized; general searches are forbidden. Here, since the officer's affidavit establishes that the defendant was being threatened, and that his cell phone was a medium for receiving the threats, the electronic search of the cell phone seized was

properly authorized. The defendant argues, however, that the search warrant was overbroad; and that the particular file in defendant's cell phone which contained his photographs ("pictures") should not have been searched. Conceding that threats could be communicated by photos attached to electronic messages (e-mail or text), the defendant nonetheless contends that such threats could, with modern forensic equipment and software used to extract data from computers and cell phones, be searched for in locations other than the defendant's personal photographs file which would be unlikely to contain evidence of threats directed to him.

It is possible, based on the testimony of defendant's expert, Mr. Nicholls, that the search could have avoided looking at defendant's "pictures" file, but still examined the cell phone for photographs that arrived by attachment to a text message. Even so, I am of the view that probable cause existed to search the "pictures" file in that particular cell phone. As reflected in the officer's affidavit, the defendant's brother told the police that the defendant informed him "that he was receiving threatening phone calls and threatening text messages on his phone." Of course searches should be limited to the locations where the items sought might possibly be located. For instance, if the defendant saved a photographic attachment which arrived by e-mail, that photograph would be found by searching the "pictures" file. E-mails were part of the officer's affidavit and application, and were covered by the search warrant. I am unpersuaded by the defendant's argument that since the defendant's brother only mentioned threatening calls and "text messages", the search warrant should not have included pictures arriving by e-mail.

Relevant case law on the subject matter has not come to my attention. The defendant recites certain principles underlying warrantless searches of automobiles set out in United States v. Ross, 456 U. S. 798, 824 (1982):

The scope of a warrantless search of an automobile thus is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of

the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.<sup>2</sup>

In this case I do not believe that the analogy to those principles is apt. Here I regard it as a reasonable possibility that evidence pertaining to "threats" could be found in the cell phone "pictures" file. I accept Mr. Nichols' testimony that it is possible for the forensic examiner to limit the retrieval to files other than the defendant's photo file, but I am satisfied that such a limitation was not constitutionally required in the case at hand.

To sum up. The affidavit furnished probable cause to conduct an electronic search of defendant's cell phone. The search warrant authorized the police to search for photographs stored in the cell phone. The scope of the search warrant was justified because threats could be conveyed by photographs. The police were, therefore, compliant with the warrant by searching the cell phone in locations where photographs were likely to be found.


The defendant does not argue that the video seized should be suppressed because "videos" are not identified as "property to be searched" under the warrant. In any event, the Commonwealth agrees that the video will not be offered in evidence as it, apparently, is not relevant.

---

<sup>2</sup> These are common sense examples which are easy for the magistrate or judge asked to approve a search warrant to apply. It is a different story when sophisticated knowledge of the architecture of a cell phone or computer are involved.

ORDER

Defendant's two motions to suppress evidence dated February 28, 2013 and March 4, 2013 are denied.

  
Patrick F. Brady  
Justice, Superior Court

14 March 13



## UNIVERSAL FORENSIC EXTRACTION DEVICE USER MANUAL

UFED Standard



UFED Ruggedized







# **UFED SYSTEM**

## **UNIVERSAL FORENSIC EXTRACTION DEVICE USER MANUAL**

This manual is delivered subject to the following conditions and restrictions:

This manual contains proprietary information belonging to CelleBrite Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the UFED.

No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of CelleBrite Ltd.

The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.

Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

Copyright 2007 CelleBrite Ltd. All rights reserved.

**WARNING:** The UFED is powered a rechargeable, Lithium Polymer battery. Please read and understand the operation and warnings before charging or using your UFED device. Improper use or charging may result in fire, personal injury, and damage to property. See Appendix A.

**WARNING:** The UFED should be used only with the dedicated AC/DC adapter supplied with this device.

**WARNING:** USB, Ethernet and target and source connectors should be connected only to CE approved devices (according to IEC/EN 60065 standard).

**WARNING:** Make sure that all external connections to other devices (except for the power adapter) are only indoor and SELV (safety extra low voltage, not exceed 42.4 V<sub>peak</sub> or 60Vdc).

## Table of Contents

<b>Chapter 1.</b>	<b>Introduction.....</b>	<b>1</b>
1.1.	Overview .....	1
<b>Chapter 2.</b>	<b>UFED Configuration: Ruggedized and Standard Versions .....</b>	<b>3</b>
2.1.	UFED Kit Contents .....	3
2.2.	UFED Device Overview .....	5
2.3.	Ruggedized UFED Carrying Case .....	6
2.4.	Ruggedized UFED Rubber Casing .....	7
2.5.	Power and Battery Options .....	8
<b>Chapter 3.</b>	<b>Getting Started .....</b>	<b>10</b>
3.1.	Initial Setup .....	10
3.2.	UFED Menu Navigation .....	11
<b>Chapter 4.</b>	<b>Extract Phone Data .....</b>	<b>12</b>
4.1.	Overview .....	12
4.2.	Flowchart .....	12
4.3.	Extract Phone Data to USB Disk Drive or SD Card.....	13
4.4.	Extract Phone Data to a PC .....	18
<b>Chapter 5.</b>	<b>Extract SIM/USIM Data.....</b>	<b>21</b>
<b>Chapter 6.</b>	<b>Clone SIM ID.....</b>	<b>23</b>
6.1.	Overview .....	23
6.2.	Flowchart .....	24
6.3.	SIM Cloning – Steps.....	24
6.4.	Manually Creating a Clone SIM Card - Steps.....	26
<b>Chapter 7.</b>	<b>Smart Phones/PDA Support.....</b>	<b>29</b>
<b>Chapter 8.</b>	<b>Using Bluetooth Connectivity .....</b>	<b>30</b>
8.1.	Phone Settings.....	30
8.2.	UFED Bluetooth Adapter .....	30
8.3.	Identifying the Phone via Bluetooth.....	30

<b>Chapter 9. UFED Report Manager Software</b>	<b>31</b>
9.1. Overview	31
9.2. UFED Report Manager Software Installation	31
9.3. Data Analysis	33
9.4. UFED Report Manager Menu	35
9.5. Reports	36
<b>Chapter 10. Services</b>	<b>39</b>
10.1. Upgrade	39
10.2. Software Versions	39
10.3. Counters	39
10.4. Help	40
10.5. Network Settings	40
10.6. Screen Settings	40
10.7. Time and Date	40
10.8. User Settings	40
10.9. UFED Settings	41
10.10 Admin Settings	42
<b>Chapter 11. Upgrade</b>	<b>43</b>
11.1. Overview	43
11.2. Upgrade from USB Disk Drive or SD Card	44
11.3. Upgrade from PC	45
11.4. Upgrade from Web	47
11.5. Automatic Upgrade from Web	49
<b>Appendix A: Battery Replacement (Ruggedized Only)</b>	<b>52</b>
<b>Appendix B: Technical Specifications</b>	<b>53</b>
<b>Cellebrite UFED System - Software Update Log</b>	<b>54</b>

## Chapter 1. Introduction

### 1.1. Overview

The Cellebrite UFED Forensics system empowers law enforcement, anti-terror and security organizations to capture critical forensic evidence from mobile phones, Smartphones and PDAs.

UFED extracts vital data such as phonebook, camera pictures, videos, audio, text messages (SMS), call logs, ESN IMEI, ICCID and IMSI information from over 1,600 handset models, including Symbian, Microsoft Mobile, Blackberry and Palm OS devices.

Cellebrite UFED enables SIM ID cloning, allowing you to extract phone data while preventing the cellular device from connecting to the network.

The UFED can extract data from a phone, or directly from the SIM card. When extracting from phone, the UFED connects to the phone via cable, Bluetooth or infrared, and the data is read logically from the phone. It also performs a physical extraction from SIM cards, allowing extraction of additional data such as deleted SMS, ICCID, IMSI, location information and more.

Data is copied to any standard USB flash drive or SD card and is then organized into clear and concise reports.

Cellebrite's industry expertise provides reliability and ease-of-use, and ensures the broadest support for handset varieties, including updates for newly released models even before they are available in the market.

Portable and easy to operate, the UFED can be used in the forensic lab as well as in the field. The UFED is a handheld device, without the need for a PC in the field. The Ruggedized version of the UFED comes with hard-sided case and battery power, for even greater mobility and flexibility and fully loaded with all needed accessories.

## Chapter 1 –Introduction

The UFED Report Manager software on your PC creates detailed reports of the extracted data that can be used as evidence. Reports include full extraction details as well as MD5 hash information that proves that the data is original and untouched.



## Chapter 2. **UFED Configuration: Ruggedized and Standard Versions**

### 2.1. **UFED Kit Contents**

The UFED comes equipped with all you need for mobile phone analysis. You can choose from either of two kit types: Standard Kit and Ruggedized Kit.

**Standard Kit**



**Ruggedized Kit**



The following table lists the features and accessories that come with each kit. Some of the accessories can be purchased separately, allowing you to upgrade some features of a Standard Kit UFED.

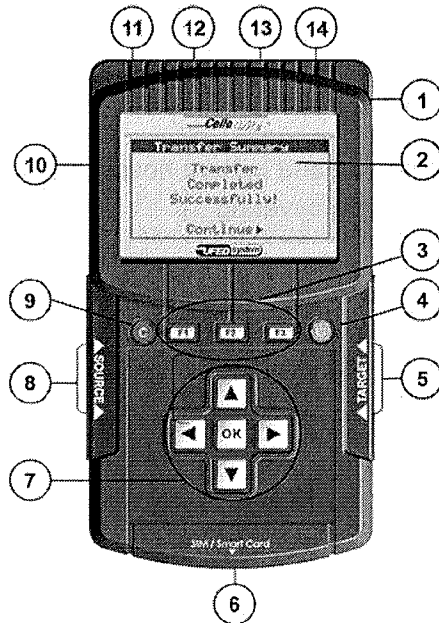


Chapter 2 –UFED Configuration:  
Ruggedized and Standard Versions

Kit Features	Standard Kit	Ruggedized Kit
Kit Carrying Case	Convenient vinyl carrying case	Hard-side plastic casing with secure latches
UFED Device	√	√
UFED Device Casing	Standard	Rubber casing with dataport flap coverings
Cable Organizer	√	√
Data Cables	Full Set	Full Set
Small Cable Pouch for quick excursions	-	√
Bluetooth Dongle for wireless phone connection	√	√
USB Flash Drive for saving examination data	√	√
AC Power Supply	√	√
UFED Battery Pack	-	√
12V In-vehicle (Cigarette Lighter) Power adapter	√	√
SIM ID Cloning Cards	√	√
Card Reader	-	√
Mobile Phone Battery Charger set	-	√
Faraday Bag	-	√
UFED Manager- Report Viewing and Printing Software	√	√
Phone Connection Cleansing Brush	√	√
User Manual and Support CD	√	√

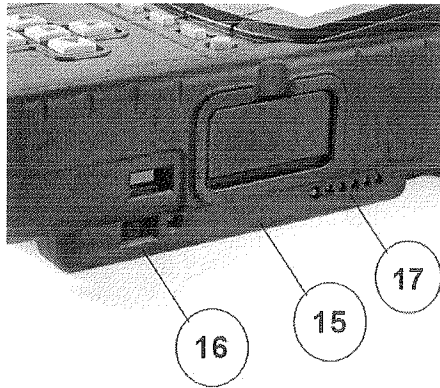
Chapter 2 –UFED Configuration:  
Ruggedized and Standard Versions

## 2.2. UFED Device Overview



1. Power Supply (Connect to power adapter)
2. LCD Display
3. Function Keys (F1 for help. F2 for select/deselect all)
4. ON/OFF Power Button
5. Target-side Connectors (For extraction to USB disk drive)
6. SIM / Smart Card Slots (Slot for reading SIM cards and smart cards)
7. Navigation Keys (For navigating the UFED menu)
8. Source-side Connectors (Connect phone via USB, serial or IR)
9. Cancel Button
10. SD Card Slot (For extraction to SD card)
11. USB Port Extension (Use for Bluetooth dongle or other external devices such as keyboard)

Chapter 2 –UFED Configuration:  
Ruggedized and Standard Versions



- 12. Serial connection (not in use)
- 13. Ethernet port (Connect to network for automatic updates and for uploading data to a network hosted PC)
- 14. Mini-USB Port (Connect to a PC via mini-USB cable, for extraction to PC)
- 15. Battery kit and battery housing protective covering
- 16. Charging switch.
- 17. Battery's state-of-charge –test and LED indicators.

### 2.3. Ruggedized UFED Carrying Case

The UFED Ruggedized carrying case is designed specifically for field use conditions.

To open the case, flip the two latches open.

NOTE: The case is air-tight sealed. When the case undergoes changes in atmospheric pressure (ex. mountain areas, after airplane flights), the latches may be 'stuck' closed. When this happens, you should release the vacuum by unscrewing the vacuum release valve, located in the center of the case, next to the handle.

Chapter 2 –UFED Configuration:  
Ruggedized and Standard Versions



#### **2.4. Ruggedized UFED Rubber Casing**

The Ruggedized UFED device is encased in a rubber casing, to hold the battery house and to protect the UFED from dirt, dust, sand or other contaminants.

To replace the casing on the UFED, refer to Appendix A.

## 2.5. Power and Battery Options

The UFED device can be powered by an AC power supply, a car power supply, or by battery power. (NOTE: car power supply and battery pack come with the Ruggedized Kit only.)

### Battery Power

To run the UFED on battery power, flip the power switch to the right (“BAT”) position. Battery power will take over.

### Charging the Battery

To re-charge the battery, connect the device to an AC adapter (supplied with the kit), and then flip the power switch to the left (“CHG”) position.

### LED Indicator

The LED indicator provides input regarding the state of the UFED power:

<u>LED Status</u>	<u>Indication</u>
Red	Battery charge in process
Green	Battery fully charged
No light	Sleep mode (no input power source) OR No battery connected OR Charge suspended (timer fault or thermal shutdown) OR Over-voltage fault
Flashing Red	Indicates a problem with the battery. Verify that the battery is connected properly.

Chapter 2 –UFED Configuration:  
Ruggedized and Standard Versions

### **Inserting or Removing Battery**

Please refer to Appendix A for instructions on installing, removing or exchanging the battery pack.

## Chapter 3. Getting Started

### 3.1. Initial Setup

#### 2.1.1 Unpacking the UFED

Unpack the UFED device from the kit (See Chapter 1). Connect the power supply adapter to the UFED. "Please Wait" appears briefly on the screen, followed by a screen showing the version numbers. When starting the UFED for the first time, you need to set the date, time and GMT. At this point, the UFED is ready to be used, and the Main Menu is displayed.



**Extract Phone Data** - This option is for extracting data from a mobile phone. (See Chapter 3)

**Extract SIM/USIM Data** – This option is physical extraction directly from a SIM card. (See Chapter 4)

**Clone SIM ID**– This option copies a SIM card, enabling you to analyze the phone without it being open for incoming calls, . (See Chapter 5)

**Services** - Allows you to upgrade your UFED with updated phone support (see Chapter 1). In addition, you can use Services to perform various administrative tasks (see Chapter 10).

## Chapter 3 –Getting Started

### 3.2. UFED Menu Navigation

The UFED shows menu options on the display.

- Use the ▲ ▼ keys to move between options.
- To select an option, press ► or the **OK** key.
- To return to the previous menu, press ◀. When additional help is available, a help icon will appear in the upper left of the screen. Press F1 to view this help.



## Chapter 4. Extract Phone Data

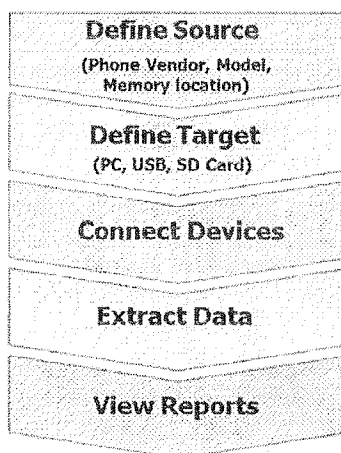
### 4.1. Overview

Select *Extract Phone Data* from the main menu in order to copy data from a phone (the source) to a PC, USB or SD card (the target).

Use this function to extract phonebook, SMS text messages, pictures, etc. from mobile phone memory to a USB disk drive, SD card or directly to a PC.

The UFED guides you each step of the way during this process.

### 4.2. Flowchart



There are only slight differences in the procedure when the target is a USB disk drive or a PC. Both procedures are described below. Refer to the procedure relevant to you.

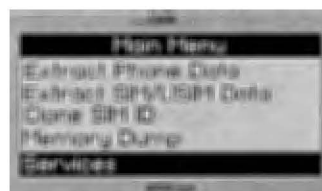
### 4.3. Extract Phone Data to USB Disk Drive or SD Card

Follow the steps below to perform a data extraction from a mobile phone to a USB disk drive or an SD card.

#### 1. Main Menu

Select *Extract Phone Data* from the main menu.

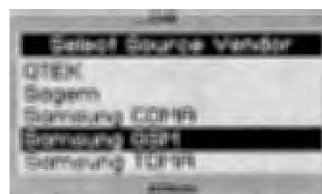
Use the ▲▼ keys to move between options. Press OK or ► to continue.



#### 2. Source Vendor

Select the vendor (manufacturer) of the source phone.

Use the ▲▼ keys to move between options. Press OK or ► to continue.



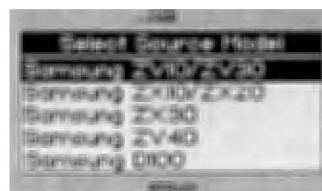
#### 3. Source Model

Select the source phone model.

NOTE: If you do not know the model, you can often find the phone model on a sticker beneath the battery.

Use the ▲▼ keys to move between options. Press OK or ► to continue.

To return to the previous menu, press ◀.

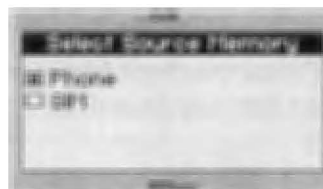


## Chapter 4 –Extract Phone Data

**4. Source Memory**

Select the source memory location you wish to extract.

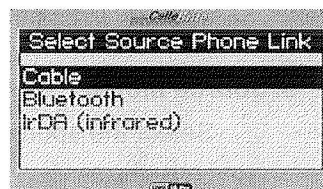
Use the ▲▼ keys to move between options. Press OK to select the currently highlighted option, or press F2 to select all. Press ► to continue.



**NOTE:** Some phones do not allow access to the SIM card data via the data cable. In these cases, you will be prompted during the process to remove the SIM card and insert it into the SIM Card Slot.

**5. Source Link**

This step determines how the phone will connect to the UFED. This message appears **only** if the phone supports more than one connection method (Cable, Bluetooth or IrDA-Infrared).



Use the ▲▼ keys to move between options. Press OK or ► to continue.

**NOTE:** For best speed and reliability, we recommend using cable whenever possible.

### 6. Target Selection

Select *USB* (or *SD*) as the target location where the content will be copied to.

NOTE: If you extract to PC, the content goes directly into the UFED Report Manager software. If you extract to USB or SD, the content is stored in a separate directory on the storage device.

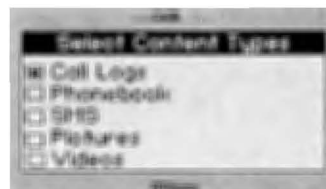
Use the ▲▼ keys to move between options. Press OK or ► to continue.



### 7. Content Types

Select content types to be extracted . The UFED displays the options according to the capabilities available in the phone. (ex. If the phone does not support video, the "Videos" option will not appear).

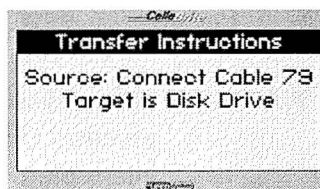
Use the ▲▼ keys to move between options. Press OK to select an option. Pressing on F2 will select/deselect all options. Press ► to continue.



### 8. Transfer Instructions: Connection

The UFED now displays the connectivity instructions.

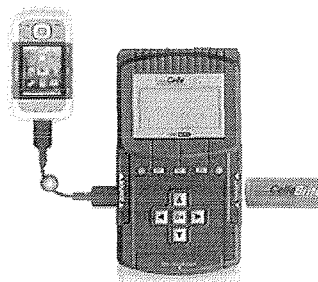
- If connecting via cable, the cable



## Chapter 4 –Extract Phone Data

number is displayed.

- If connecting via Bluetooth, refer to Chapter 6 for details.
- If connecting via IrDA (Infrared), place the phone with its infrared port directly in front of the UFED's source or target infrared port.



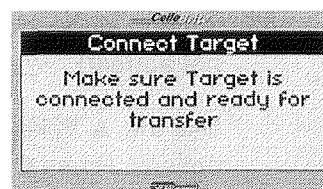
Make sure that the phone is powered on, and the data connector is clean.

NOTE: When connected to the UFED, some phones will prompt you to choose an operating mode, such as "PC Suite" or "Phone Mode".

Press ► to start extraction.

### 9. Connect Target Device

If you have not yet plugged the USB drive or SD card into the UFED, do it now. The UFED is ready to copy the data to the storage device.



Press ► to continue.

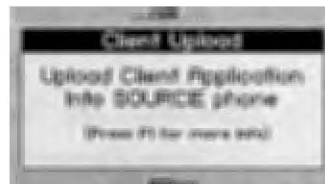
**WARNING:** Do not disconnect the phone or the power adaptor during the process! Once started, the process should not be interrupted.

## Chapter 4 –Extract Phone Data

**10. Smartphone / PDA Installation**

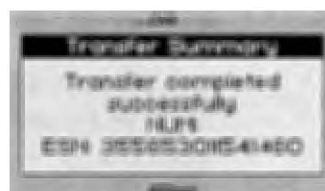
If the phone is a Smart Phone or PDA, you may need to install a client application on the phone.

Press ► to continue.

**11. Completion**

Upon the completion of the process the UFED- displays a message.

The message on the screen includes the phone's ESN (for CDMA) OR IMEI (for GSM).



NOTE: Besides the standard user phone data, the UFED also provides metadata about the phone. Among this data is the ESN (for CDMA phones) or IMEI (for GSM phones). The ESN or IMEI is a unique identifier or serial number uniquely associated with each single handset device.

At this stage, the data is stored on the USB drive. This backup directory can be opened in the UFED Report Manager PC software to analyze data and generate reports. The data is also stored in HTML format, and can be opened on any PC.

The transfer process is complete and you may now disconnect the phone and the PC from the UFED device.

#### 4.4. Extract Phone Data to a PC

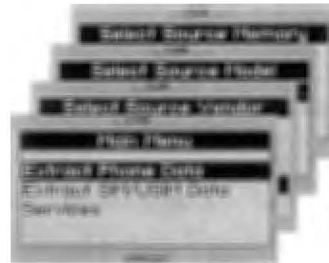
The UFED system includes UFED Report Manager software, which you can use to upload the extracted phone data from the UFED to your PC.

##### 1. Main Menu and Phone Definitions

Select *Extract Phone Data* from the main menu, and then select the phone vendor, model, memory location and link method.

This part of the process is identical to the USB Extraction process. (see Section 4.3).

Use the ▲▼ keys to move between options. Press OK or ► to continue.



##### 2. Target Selection

Select *PC* from the target menu.

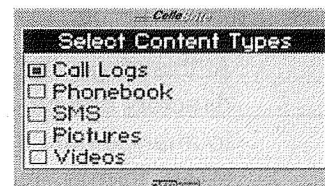
Use the ▲▼ keys to move between options. Press OK or ► to continue .



##### 3. Content Types

Select content types to be extracted. The UFED displays the options according to the capabilities available in the source phone. (ex. If the phone does not support video, the “Videos” option will not appear).

Use the ▲▼ keys to move between options. Press OK to select an option.



## Chapter 4 –Extract Phone Data

Press ► to continue.

NOTE: Transfer time varies according to the data types selected.  
Selecting all options will increase the transfer time.

#### 4. Transfer Instructions: Connection

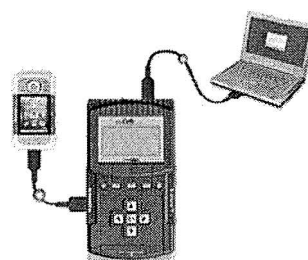
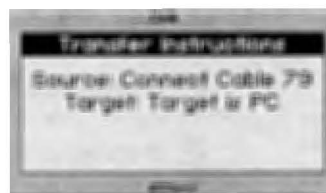
Make sure that the UFED is connected to the PC using the mini-USB cable.

The UFED displays the cable number to be used to connect the phone.

NOTE: When connected to the UFED, some phones will prompt you to choose an operating mode, such as "PC Suite" or "Phone Mode".

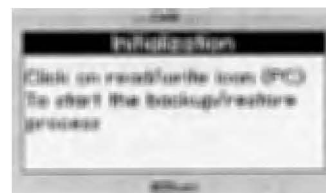
Press ► to continue.

The UFED now extracts the selected data to its internal memory, the following message will appear at the end of the extraction:



#### 5. Run the UFED Report Manager

Run the UFED Report Manager software on your PC by choosing Start/Programs/Cellebrite Mobile Synchronization/UFED Report Manager.





## Chapter 4 –Extract Phone Data

### 6. Read Data from Phone

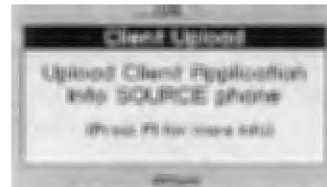


Click the Read phone icon.

- If connecting the phone via cable, the UFED informs you which cable number to use. Find the cables in the cable organizer, according to the numbers indicated on the cable.
- If connecting via Bluetooth, refer to Chapter 6 for details.
- If connecting via IrDA (Infrared), place the phone with its infrared port directly in front of the UFED's source or target infrared port.

### 5. Smartphone / PDA Installation

If the extracted phone is a Smart Phone or PDA, you may need to install a client application on the phone. (See Chapter 7)



Press ► to continue.

### 6. Transfer

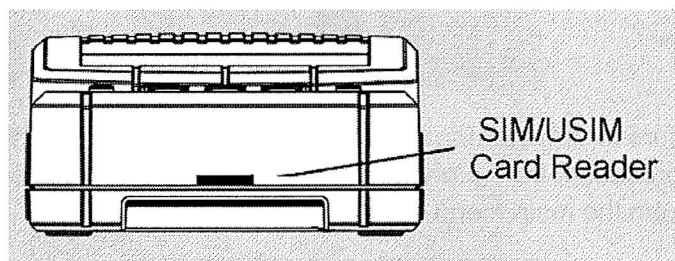
The UFED now sends the extracted data from its internal memory to the PC.

Transfer process is complete and you may now disconnect the phone and the PC from the UFED device.

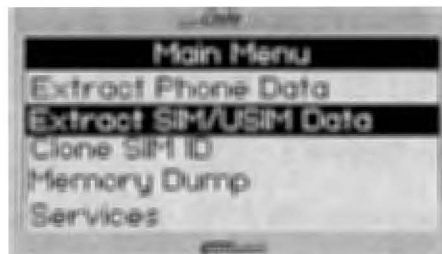
## Chapter 5. Extract SIM/USIM Data

Your UFED is equipped an integrated SIM/USIM card reader. It is located at the bottom of the UFED, as shown below.

*FRONT VIEW OF UFED DEVICE*



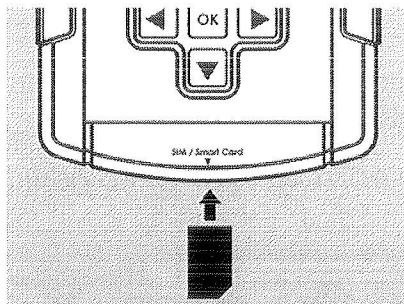
You can use this SIM reader to extract data directly from the SIM card instead of via the phone, or when the SIM card is not accessible via the phone.



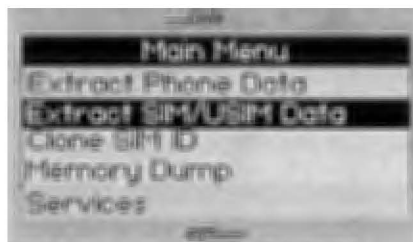
Using the second option from the main menu gives the option of Physical extraction and the output of this extraction is additional data from the SIM such as ICCID, IMSI, location information, SMS, deleted SMS, Phonebook and more.

When using the SIM Card Reader, insert the SIM as shown in the picture below. Be sure that the angled side is on the outer side. The actual SIM contacts should be facing down.

## Chapter 5 –Extract SIM/USIM Data



The procedure for transferring data to a SIM card is similar to the data extraction procedure from a phone described in Chapter 4. Select *Extract SIM Data* from the main menu.



Insert the SIM card as described above, and continue exactly as described for phone extraction in Chapter 3.

**NOTE:** If the SIM is protected with a PIN, you will need to enter the PIN during the transfer process. To enter the PIN code, use the ▲▼ keys to move the cursor to the required digit, and press OK to select that digit. Repeat this for each digit of the PIN. To delete a digit, press the © key. When complete, press F3

## Chapter 6. Clone SIM ID

### 6.1. Overview

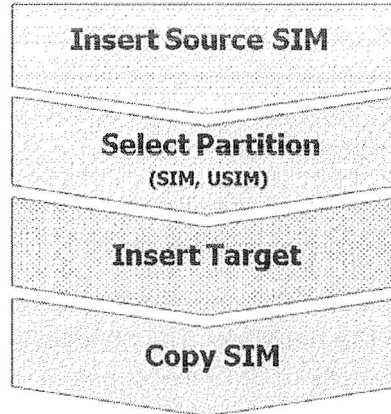
Cellebrite's UFED (Universal Forensics Extraction Device) is capable of SIM ID Cloning utilizing the existing built in SIM Reader, providing your organization with valuable new functionality.

The SIM ID Cloning capabilities of Cellebrite's UFED System solve many key problems facing forensic examiners today:

- **Extract Phone data while preventing the cellular device from connecting to the network-** The handset will be invisible to the network with no calls or SMS messages to, or from the handset, preserving the current call and SMS history in the device- No Faraday Bag required to block RF signals
- **Extract Phone data when the original SIM is not available-** ICCID or IMSI can be manually programmed into the Cloned SIM ID Card to mimic the original missing card
- **Extract Phone data when the SIM card is PIN locked -** Cloning the identification of the original SIM, allows the phone data to be extracted without losing critical data including call history and SMS's.

## Chapter 6 –Clone SIM ID

## 6.2. Flowchart

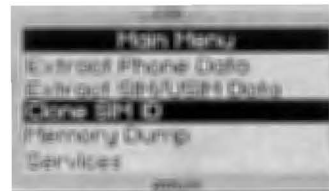


## 6.3. SIM Cloning – Steps

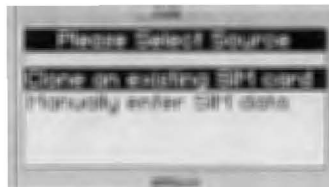
**1. Main Menu**

Select *Clone SIM ID* from the main menu.

Use the ▲▼ keys to move between options. Press OK or ► to continue.

**2. Select Source**

Select *Clone an existing SIM Card* from the Select Source menu.

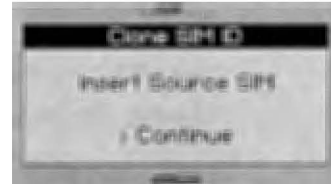
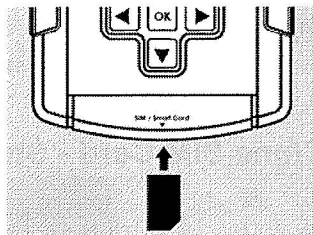


## Chapter 6 –Clone SIM ID

**3. Insert Source SIM**

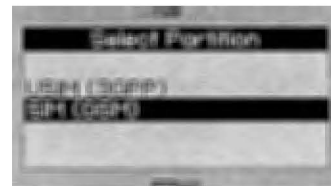
Insert the SIM card that you wish to clone, with the gold side facing down and the cut corner facing outwards.

The slot for the SIM card is located at the bottom of the UFED device.

**4. Select Partition to Read**

If the card is a 3G SIM card, you will next be asked to choose the partition.

Use the ▲▼ keys to move between options. Press OK or ► to continue.

**5. Insert Target Card**

The UFED device now reads data from the source SIM card, storing it in its internal memory.

The UFED then asks you to insert the target card. Insert the UFED SIM ID blank card and press ► to continue.

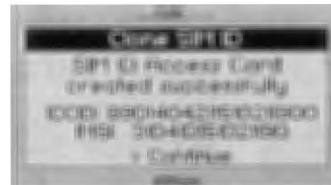


**6. Finished**

The UFED next completes the SIM Cloning process.

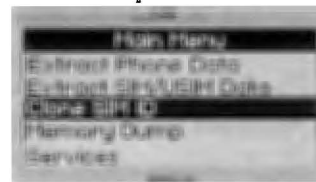
ICCID and IMSI data is shown on screen.

At this point, you can insert the cloned SIM card into the phone, and continue evaluating the phone.

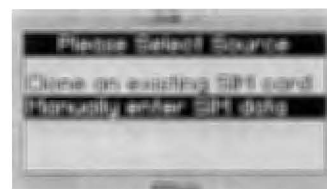
**6.4. Manually Creating a Clone SIM Card - Steps****1. Main Menu**

Select *Clone SIM ID* from the main menu.

Use the ▲▼ keys to move between options. Press OK or ► to continue.

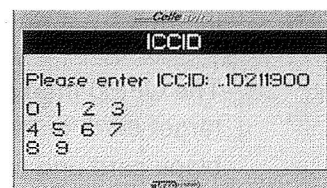
**2. Select Source**

Select *Manually enter SIM data* from the Select Source menu.

**3. Enter ICCID and IMSI**

When prompted, enter the ICCID number and the IMSI number.

Use the arrow keys to highlight a digit. Press OK to add the digit. Press F3 when finished.

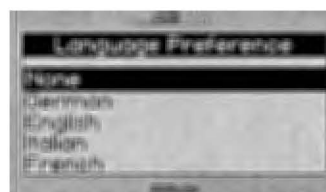


## Chapter 6 –Clone SIM ID

**4. Language Preferences**

Optionally, you may specify the default language preference for the SIM card.

Use the ▲▼ keys to move between options. Press OK or ► to continue.

**5. Advanced Settings**

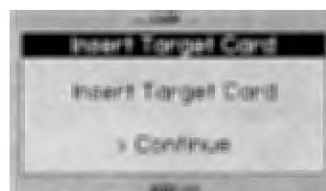
If you wish to add SPN, GID1 and GID2 settings to the SIM card, select Yes at the Advanced Settings menu. Otherwise, select No.

Use the ▲▼ keys to move between options. Press OK or ► to continue.

**6. Insert Target Card**

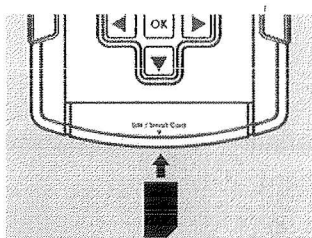
The UFED then asks you to insert the target card. Insert the Cellebrite UFED SIM ID blank card into the SIM reader, with the gold side facing down and the cut corner facing outwards and press ► to continue.

The slot for the SIM card is located at the bottom of the UFED device.





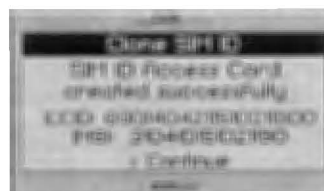
## Chapter 6 –Clone SIM ID

**7. Finished**

The UFED next completes the SIM Cloning process.

ICCID and IMSI data is shown on screen.

At this point, you can insert the cloned SIM card into the phone, and continue evaluating the phone.



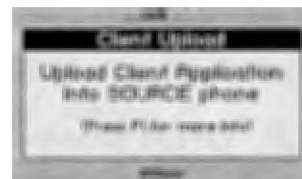
## Chapter 7. Smart Phones/PDA Support

When extracting data from Smart Phones or PDA's, you will be asked to upload a client application from the UFED to the phone. This application enables access to the phone memory.

NOTE: Application upload is not necessary for Blackberry and Symbian 3<sup>rd</sup> edition phones.

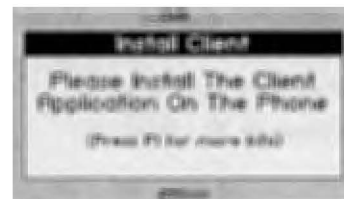
### 1. Client Upload

When necessary, the UFED will inform you to upload the client application, as follows.




### 3. Install Client Prompt

The UFED now instructs you to run the installation on the phone.



### 4. Install and Run the client

If the phone prompts you to install, follow the installation steps. Then run the application. You can identify it by the  icon.

**Pressing F1 on the UFED will inform you of the exact location where the program can be found on the phone.**

NOTE: After completing the entire extraction process, you can uninstall the client from the phone.

## Chapter 8. Using Bluetooth Connectivity

On some phones, the UFED enables you to use Bluetooth instead of data cables for the extraction process. When you choose Bluetooth for the connectivity type, follow these instructions:

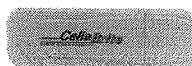
### 8.1. Phone Settings

On the mobile phone, you must enable the phone to connect via Bluetooth, by turning Bluetooth capabilities on.

In addition, you must set the Bluetooth services to 'Visible' on the phone.

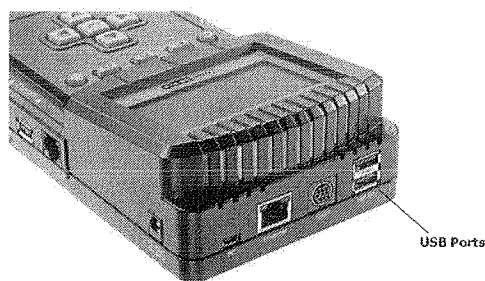
### 8.2. UFED Bluetooth Adapter

The UFED kit comes with a Bluetooth USB adapter, as shown.



Insert the Bluetooth adapter in either of the two USB ports at the top of the UFED, as shown.

Press ► to continue.



### 8.3. Identifying the Phone via Bluetooth

The UFED searches for visible Bluetooth devices within its proximity, and provides a list of all devices that it finds. Select the appropriate device from this list. Use the ▲ ▼ keys to move between options. Press ► to continue. The UFED then instructs you to enter "0000" in the phone to complete the pairing between the devices. Once doing this, all data transfer between the UFED and the phone will be performed using Bluetooth.

## Chapter 9. UFED Report Manager Software

### 9.1. Overview

The UFED System includes UFED Report Manager Software, which you can use to view and analyze the extracted data on your PC.

The UFED Report Manager enables you to:

1. View and analyze the data extracted.
2. Print a detailed report of the extracted content.
3. Save extracted data.

Throughout the report, data is shown with its full MD5 hash information. When extracting pictures, audio and video files, the UFED system calculates an MD5 hash of each file. The MD5 hash provides a tamper-proof signature of the source file. Any modifications to the file will cause the MD5 hash to change. In this way, the MD5 hash proves the authenticity of each file.

### 9.2. UFED Report Manager Software Installation

The following steps will guide you through the UFED Report Manager installation process.

#### *1. Install UFED Report Manager software on PC*

In order to install the UFED Report Manager, first make sure that Microsoft Dot Net 2.xx is installed on your PC. If it is not, you can find the dotnetfx.exe file on the Cellebrite CD. Install this file and follow the installation instructions.

Next, click on the UFED Report Manager *setup.exe* and follow the installation instructions.

## Chapter 9 –UFED Report Manager Software

### 2. Run UFED Report Manager on PC

Launch the UFED Report Manager program on your PC. It can be found on the *Start* menu under *Programs / Cellebrite Mobile Synchronization/ UFED Report Manager*.

### 3. Connect the UFED to the PC using mini-USB cable

Use the mini-USB cable that comes in the UFED kit to connect the UFED device to your computer. The small end of the cable connects to the UFED mini-USB port, labeled *PC*.



**NOTE:** The connection between the UFED device and the PC is necessary only if you will be performing extractions directly to PC. If you perform extraction to USB or SD card, you do not this connection.

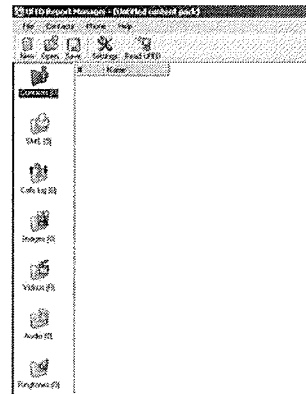
## UFED Device Driver Installation

A USB device driver is necessary in order for the PC to recognize the UFED device. In most cases, Windows will automatically pop up a window, asking to install the device driver. Insert the installation CD in the CD drive of the computer, and follow the steps of this wizard, selecting *Find on Installation CD*.

Launch the UFED Report Manager program on your PC. It can be found on the *Start* menu under *Programs / Cellebrite / UFED Report Manager*.

### 9.3. Data Analysis

The following icons are shown on the left of the window. Under each icon, the number of items of each type is shown



The Optional Information Icon allows you to enter any optional or mandatory fields, as specified in the Tools Settings. This data is then included in the report.



The Report icon shows the full set of information in HTML format with links to any sections.



The Contacts icon shows the phonebook contacts list, in tabular format. The table is sortable by clicking on each column header.



The SMS icon shows all SMS messages sent and received with time stamp for each message.



Call log shows all Outgoing, Incoming and Missed calls with time stamp for each call. The UFED automatically associates a name to each phone number, if that number exists in the phonebook contacts. This association is valid only in the context of the current state of the phonebook at time of extraction.



The Images icon shows a thumbnail view of each image.



The Videos icon shows a thumbnail view of each video.

## Chapter 9 –UFED Report Manager Software



The Audio icon gives a list of each audio file.



The Ringtones icon gives a list of each ringtone.

## 9.4. UFED Report Manager Menu

### File

Open Content Pack	Opens a content pack that has been previously saved on the computer. The file format of a content pack is *.ucp.
Save Content Pack	Saves the currently open data in a content pack file (*.ucp)
Save Content Pack as	Saves the currently open data in a content pack file (*.ucp) in a new location or different name
Print preview	Displays the full content report on screen in the format that it will be printed.
Print	Sends the report to a printer.
Auto Updates	Cellebrite occasionally distributes updated versions for the UFED Report Manager software. For your convenience, you can set your PC to automatically check the network for new updates.

### UFED

Read from UFED	Upload extracted data from the UFED memory to the PC. Select this option when the UFED device instructs you to do so.
----------------	---



## Chapter 9 –UFED Report Manager Software

**Tools**

Settings	Change the default settings of the contacts in the report (Last name/first name order), for viewing or printing purposes.
UFED Settings	Choose formatting options for forensic reports, and specify optional information to be included in reports.
Help	Displays basic information about the software version.

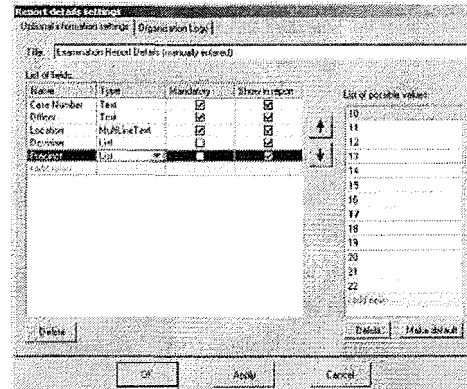
**9.5. Reports****Forensics Settings**

Selecting Forensics Settings on the Tools menu allows you to configure the formatting and layout of the UFED reports, and also enables you to specify general information fields (ex: Inspector's Name, Case Number, Department etc.) that the user adds to each report.

On the Optional Information Settings tab, enter any fields that you want to include in each report. For each field, you specify the following characteristics:

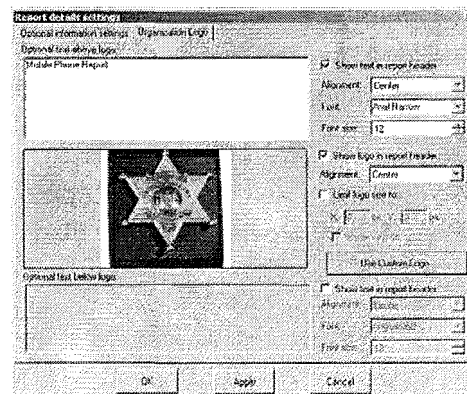
## Chapter 9 –UFED Report Manager Software

- Name – The name of the field as it will appear in the report
- Type – Choose between Text, Multi-Line Text or List. If it is a List, you also specify the possible values of the list and the default value, in the field on the right of the window.



- Show in report– Specifies whether to show this field in the report.
- Mandatory – If the field is enabled, then this specifies if the field must be filled in by the user, or if it is optional and can be left blank.

On the Organization Logo tab, you can design the report header formatting. Specify a logo to appear in the header, and add text to appear above and below the logo.



### Entering Optional Information

According to the settings defined in the Forensics Settings screen, the user will be prompted for the optional information when producing a report. Click on the *Optional Information* tab, and enter the information in the fields provided. Mandatory fields are marked with a \*

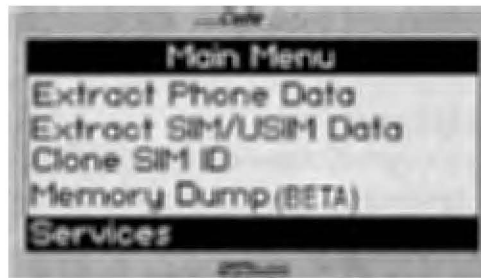
### Viewing and Printing Reports

At any stage, you can view and print reports. Click on the *Report* icon on the left side of the window. The report contents appear on the screen.

To print the report, choose *Report / Print*. A print preview option is also available.

## Chapter 10. **Services**

The Services option on the main menu allows you to perform various administrative tasks for the UFED.



### **10.1. Upgrade**

The Upgrade process enables you perform software upgrades for the UFED. This process is detailed in full in Chapter 1.

### **10.2. Software Versions**

Displays the current version numbers and system information.

- App – The application version
- Full and Tiny – The software image versions
- S/N – The UFED Serial Number
- ID – The unique identifier, used during the activation process

### **10.3. Counters**

- Show Counters - Shows the number of transactions performed by the UFED device
- Reset Counters - Resets all counters to zero
- Set Counters - Allows you to set the counters to a specific value

### 10.4. Help

- **Phone Specific Help** - Allows you to view various help information about specific phones
- **Generate File** – Allows you to generate and export the full help info to a USB disk drive

### 10.5. Network Settings

Allows you to configure various network settings for the UFED device, when connected to a network via the Ethernet port. Press F1 for configuration.

Settings include:

- **Dynamic IP settings** – Dynamic or Static DNS
- **Static IP settings** – IP addresses

### 10.6. Screen Settings

- **Contrast** - Modify the contrast level of the LCD screen

### 10.7. Time and Date

Set the current time and date on the UFED device including GMT and Daylight saving time

### 10.8. User Settings

#### User interface

- **Select Language** – Change the menu language
- **Silent Mode** – Mutes all UFED sounds
- **Failure Notification** –Beeps when a UFED operation fails.
- **Connect Device Prompt** - UFED prompt to connect the target device after the "reading" process. Turning this feature off will

## Chapter 10 – Services

save time by eliminating prompts during the extraction process.

- **Estimated Transfer Time** - Turns on or off the extraction time estimation, which appears during the extraction process.
- **Help Instructions** – Sets how to expose the "help" instructions to the user.

### **Global Settings**

- **Create Log file**
- **Restore Factory Defaults** - Reset the UFED to the original factory settings

### **Phonebook Setting: Name Order**

- Change between "LastName FirstName" and "FirstName LastName" ordering when copying phonebook data

## **10.9. UFED Settings**

### **Report Information**

- If these options are enabled, it allows you to enter free text such as case/file number, examiner's name, department, location and notes to be added to each transfer process as part of the report. The user will be prompted during the transfer process to enter the values for these fields. This data will automatically be added to the Examination Report.

NOTE: The UFED Report Manager software also enables users to add various fields to each report.

## Chapter 10 – Services

### Mobile Client Settings

- **Client Covert mode** – Rename the application client name from "Cellebrite.sis/exe" to "AAA.sis/exe".

**Client Uninstall Reminder** – When enabled, the UFED will prompt the user to uninstall the client from the examined smartphone.

### Report Settings

- **Report Format** – Change the layout of the HTML report to compact mode or normal mode.
- **Generate XML Report** – Enabling this feature will add a report in XML format to the target.

## 10.10 Admin Settings

\*The password for this section is: ADMIN333

- **Global Settings**– Enable Report and Help menu
- **Users List** – Manage users in white list to work with the UFED
- **Crime Types List** – Enable to add crime category to the report

## Chapter 11. Upgrade

### 11.1. Overview

Cellebrite continuously updates its UFED software, providing support for new phone devices as they are released by the various phone vendors. The Upgrade process installs these various updates on your UFED device.

The UFED application is constructed of three main files:

1. Tiny Image – Core system software
2. Full Image – Additional core system software
3. Application – The UFED application and data, including support for the various phone models.

When upgrading, you choose either Application Upgrade or Images Upgrade. The Images Upgrade option updates both the Full and Tiny images.

You can upgrade your UFED in one of three ways:

1. Locally via USB Disk Drive or via SD card
2. Locally via PC
3. Remotely via the Internet

Automatic upgrade can be done when the UFED is connected to the internet, via the Ethernet connection.

**NOTE:** When performing an upgrade, the UFED will reset itself. Do not interrupt the process at any stage. The full upgrade process takes approximately four minutes.



## Upgrade

**11.2. Upgrade from USB Disk Drive or SD Card****1. Main Menu**

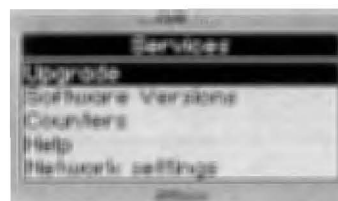
Select Services.

Press OK or ► to continue.

**2. Services Menu**

Select Upgrade.

Press OK or ► to continue.

**3. Upgrade Menu**

For a manual upgrade, you have two options:

- Upgrade Application Now – The 'application' refers to the UFED application data, which includes the support information for any new phones.
- Upgrade Image Now – The 'image' refers to the core software that is running on the UFED.



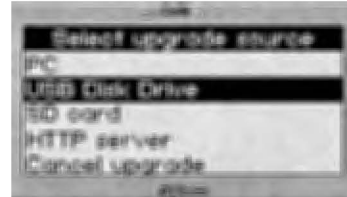
Use the ▲ ▼ keys to move between options. Press OK or ► to continue.

## Chapter 11 - Upgrade

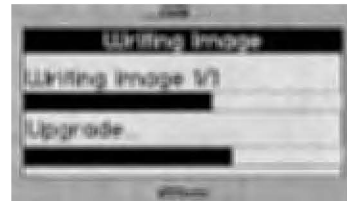
**4. Select Upgrade Source**

Choose USB Disk Drive or SD Card, according to where you have copied the upgrade files.

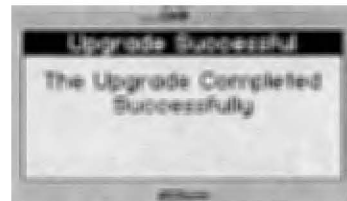
Use the ▲ ▼ keys to move between options. Press OK or ► to continue.

**5. Upgrade**

The UFED will display the available upgrade files. Select the correct file, Press OK or ► to continue The UFED now performs the upgrade. Do not interrupt the UFED until the full process is complete.

**6. Finish**

After finishing the upgrade process, the UFED displays a message indicating that it completed the update. It will then restart automatically, and return you to the main menu.

**11.3. Upgrade from PC**

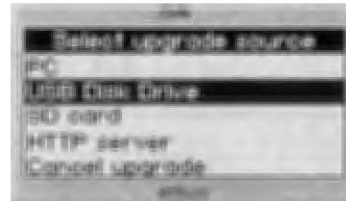
In order to upgrade from PC, the Upgrade Utility is required on your PC. If it is not already installed, run the installation located on the CD in the UFED Kit.

## Upgrade

When upgrading from a PC, the process is similar to that described above for USB Disk Drive, with a few additional steps on your PC, as described below.

### 1. Select Update Type and Source

On the UFED, after choosing *Services / Upgrade*, choose the type of upgrade (Application or Image) and select *PC* as the source for the upgrade.



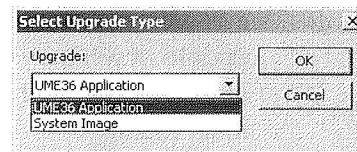
Use the ▲▼ keys to move between options. Press OK or ► to continue.

### 2. Run the Upgrade Program on the PC

Run the Upgrade Program, via "Start / Programs / Cellebrite / Upgrade Program."

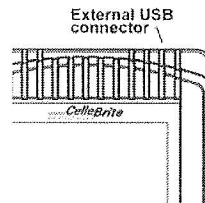
### 7. Select Upgrade Type

On your PC, select the upgrade type, according to the type that you chose in step 1



### 8. Connect the UFED to the PC

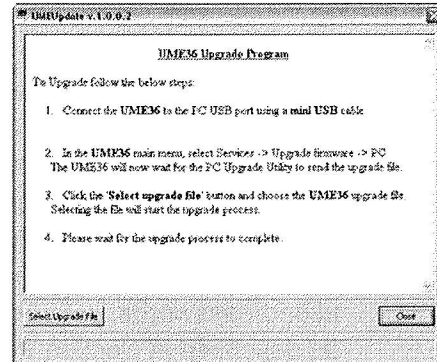
Connect your UFED to the PC using the mini-USB cable provided in the kit. The cable connects to any standard USB port on the PC.



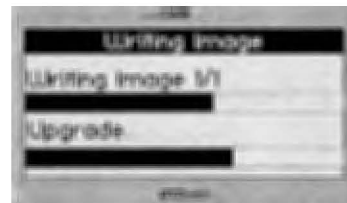
## Chapter 11 - Upgrade

**9. Start the upgrade process**

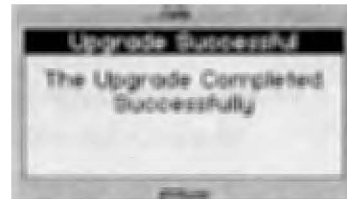
Start the upgrade process by performing the steps that are requested by the software's dialog box displayed on your PC.

**10. Upgrade**

The UFED now performs the upgrade. Do not interrupt the UFED until the full process is complete.

**11. Finish**

After finishing the upgrade process, the UFED displays a message indicating that it completed the update. It will then restart automatically, and return to the main menu.

**11.4. Upgrade from Web**

## Upgrade

**1. Configure HTTP Settings (one time only)**

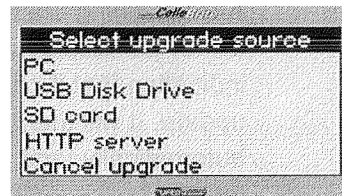
To upgrade from the web, first make sure that the FTP/HTTP settings are initialized properly. For most network environments, the UFED comes preconfigured properly. In some cases where network environments require proxies and userid/passwords, set these settings as described in Section 11.5

**2. Connect the UFED to the network**

Connect the UFED device to your network via the Ethernet port on the top of the UFED. Use a standard Ethernet cable for this connection.

**3. Select Update Type and Source**

On the UFED, after choosing *Services / Upgrade*, choose the type of upgrade (Application or Image) and select *HTTP Server* as the source for the upgrade.

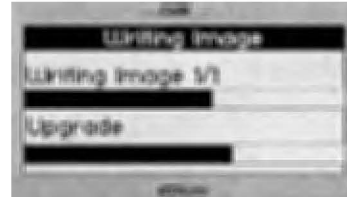


Use the ▲▼ keys to move between options. Press OK or ► to continue.

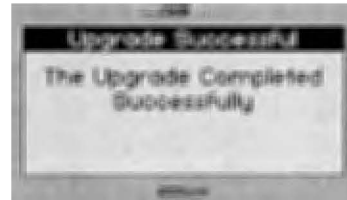
## Chapter 11 - Upgrade

**4. Upgrade**

The UFED now performs the upgrade, by fetching the upgrade files from the HTTP server. Do not interrupt the UFED until the full process is complete.

**5. Finish**

After finishing the upgrade process, the UFED displays a message indicating that it completed the update. It will then restart automatically, and return to the main menu.

**11.5. Automatic Upgrade from Web**

If your UFED is connected to the network via the Ethernet port, you can configure it to perform automatic upgrades. This enables you to keep your UFED up-to-date without requiring any ongoing interaction.

We recommend using this method, as it eliminates the manual process for each upgrade, and guarantees that your UFED remains up to date.

To do this, first select Upgrade Settings from the Upgrade menu. Then, set the following settings according to your preferences and your network requirements, as described in the following section.

## Upgrade

Auto Upgrade:  
Method

- Disabled – The UFED will not perform any automated upgrades
- FTP – The UFED will access an FTP site in order to get upgrade files
- HTTP – The UFED will use HTTP to access upgrade files

Auto Upgrade:  
Period

Choose how often you want the UFED to check for upgrades – Daily, Weekly or Monthly.

## FTP Settings

If you chose FTP for your upgrade method, specify the ftp details, as provided by your distributor. You will need to specify:

- FTP Address
- Port Number
- Username
- Password

Hit F3 after each screen in order to continue.

FTP Proxy  
Settings

- Direct Connect – Choose this if your network security does not require a proxy to access external FTP sites.
- Use Proxy – If a proxy is needed, choose this option. You will then be asked to provide the address and port of the proxy

Chapter 11 - Upgrade

HTTP Settings      Similar to the FTP settings, when the upgrade method is HTTP

HTTP Proxy Settings      Similar to FTP Proxy settings, when the upgrade method is HTTP.

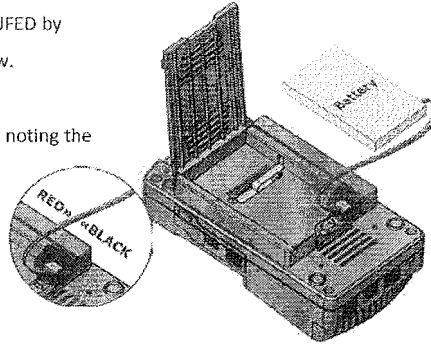
- App – The application version
- Full and Tiny – The software image versions
- S/N – The UFED Serial Number
- ID – The unique identifier



## Appendix A: Battery Replacement (Ruggedized Only)

**Appendix A: Battery Replacement (Ruggedized Only)**

1. Open battery compartment located on the back of the UFED by pushing on the release latch in the direction of the arrow.
2. Attach connector:
  - a. Remove the old battery and unplug the connector, noting the orientation of the connector.
  - b. Connect the new battery, taking care to connect the power connector in the same orientation.
  - c. Place the battery in the battery box.
  - d. Close the cover
  - e. Check UFED power by sliding the power switch to 'BAT' (unit should power on if battery is charged), Charge the device if necessary, by connecting it to the power supply, and sliding the power switch to 'CH'



**Warning:** Lithium Polymer batteries are volatile. Improper use, or charging may result in fire, personal injury, and damage to property.

**Warning:** The batteries could be used within the following temperature ranges. Exceeding these ranges could result in fire, personal injury, and damage to property

- Operating Temperature: -20 to 60°
- Storage Temperature: -20 to 45° for 1 Month.  
(Storage temperature for longer periods should be limited to: 0 to 25°C)
- Charging Temperature: 0 to 45°

**Warning:** Over-discharging of Li-Polymer cells can cause cell degradation, functional losses, and battery swelling. The cells can degrade into an over-discharge state through self discharging.

**Battery over-discharging prevention- precautionary measures:**

1. When the UFED battery charge drops below 15% (all indication LEDs are off), charge the device as soon as possible.
2. The slide switch should never be left in 'BAT' position if the UFED is not in use. Prolonged time in this setting (1 month +) can result in damage the battery and reduce capacity.
3. Check the batteries capacity periodically and charge when necessary.

## Appendix B: Technical Specifications

<b>Appendix B: Technical Specifications</b>
---

Power Supply (UFED Ruggedized) :	Input: AC 100-240V, 50/60Hz Output: DC 15V, 3.3A
Power Supply (UFED Standard) :	Input: AC 100-240V, 50/60Hz Output: DC 12V, 2A
Interfaces:	RJ-45 (source phone) RJ-45 (target side) USB (source phone) USB (target phone) Mini DIN to PC COM Port SIM reader IrDA (source and target)
IRDA	2 Infrared transceiver modules. Supports STD IrDA speeds (up to 115kbps)
Ethernet controller	LAN91C111, 10/100MBPS Ethernet- controller, and an 8KB packet buffer SDRAM
CPU	Intel XScale micro-architecture
CPU frequency	520MHz
Bus frequency	104MHz Memory Capacity
SD RAM	128MByte (RAM)
Flash memory	Intel StrataFlash embedded memory 64MByte density
Operating System	Microsoft Windows CE
Operating Temperature:	0°C to 70°C / 32°F to 158°F
Storage Temperature:	-40°C to 80°C / -41°F to 176°F
Battery Maintenance:	<b>Operating Temperature</b> (Discharge): -20~60° <b>Storage Temperature:</b> -20~45° for 1 Month. -20~35° for 12 Months <b>Charging Temperature:</b> 0~45° (Cycle life: ≥300)
Maximum relative humidity	95%

## Cellebrite UFED System - Software Update Log

Cellegre releases software updates frequently to support new phone devices, as well as add feature functionality. It is extremely important to update your UFED on a regular basis to maximize it's capability to support all the latest mobile devices available.

Software updates are emailed from Cellebrite monthly to contacts on an email distribution list. If your organization is not receiving updates on a regular basis, would like to add additional emails for distribution, need instructions, or technical support for the process, please contact Cellebrite

[illegible]

