

---

IN THE SUPREME COURT OF THE STATE OF OREGON

STATE OF OREGON,  
Plaintiff-Appellant,  
Respondent on Review,

v.

JAMES TYLER NIX,  
Defendant-Respondent,  
Petitioner on Review.

Linn County Circuit Court  
Case No. 07122775

CA A138483

SC S058751

---

**BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER  
FOUNDATION IN SUPPORT OF PETITIONER JAMES TYLER NIX**

Review of the Decision of the Court of Appeals  
On an Appeal from the Judgment  
Of the Circuit Court for Linn County  
for the State of Oregon  
Honorable RICK J. MCCORMICK, Judge

Affirmed with Opinion: June 23, 2010  
Reversed and Remanded

Author of Opinion: Haselton, PJ

By: Haselton, Presiding Judge, Armstrong, Judge, and Deits, Senior Judge

ELECTRONIC FRONTIER  
FOUNDATION  
Marcia Hofmann, Esq.  
(CA State Bar. No. 250087)  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
(415) 436-9993 (fax)

CREIGHTON & ROSE, PC  
J. Ashlee Albies, Esq.  
(OR State Bar No. 05184)  
815 SW Second Ave, Suite 500  
Portland, OR 97204  
(503)221-1792  
(503) 223-1516 (fax)

*Attorneys for Amicus Curiae*

**TABLE OF CONTENTS**

TABLE OF AUTHORITIES.....	iii
STATEMENT OF AMICUS CURIAE .....	1
SUMMARY OF ARGUMENT.....	2
ARGUMENT .....	2
I. People Have A Strong Expectation Of Privacy In The Information Stored On Their Cell Phones And Other Portable Digital Devices. ....	4
II. The Search-Incident-To-Arrest Doctrine Does Not Legitimize The Warrantless Search Of The Entire Contents Of A Cell Phone. ....	8
A. The Search-Incident-To-Arrest Exception Does Not Apply Where Officer Safety, Evidence Destruction Or Other Exigencies Are Not Concerns. ....	9
B. No Exigency Exists To Justify The Routine Warrantless Search Of Cell Phones Incident To Arrest.....	16
CONCLUSION.....	19

## TABLE OF AUTHORITIES

### CASES

<i>Arizona v. Gant</i> , __ U.S. __, 129 S. Ct. 1710 (2009).....	passim
<i>Chimel v. California</i> , 395 U.S. 752 (1969).....	3, 9, 10, 11
<i>Connecticut v. Boyd</i> , 992 A.2d 1071 (Conn. 2009).....	4
<i>Katz v. United States</i> , 389 U.S. 347 (1967) .....	3, 4
<i>Ohio v. Smith</i> , 920 N.E.2d 949 (Oh. 2009).....	4, 16
<i>People v. Diaz</i> , 244 P.3d 501 (Cal. 2011).....	12
<i>Stanley v. Illinois</i> , 405 U.S. 645 (1972).....	18
<i>Trupiano v. United States</i> , 334 U.S. 699 (1948) .....	11
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977).....	passim
<i>United States v. Comprehensive Drug Testing</i> , 621 F.3d 1168 (9th Cir. 2010)..	3
<i>United States v. Edwards</i> , 415 U.S. 800 (1974).....	12, 13, 14
<i>United States v. Feldman</i> , 788 F.2d 544 (9th Cir. 1986).....	9
<i>United States v. Finley</i> , 477 F.3d 250 (5th Cir. 2007).....	4, 12
<i>United States v. James</i> , No. 1:06CR134 CDP, 2008 U.S. Dist. LEXIS 34864 (E.D. Mo. April 29, 2008).....	18
<i>United States v. Karo</i> , 468 U.S. 705 (1984).....	18
<i>United States v. Mercado-Nava</i> , 486 F. Supp. 2d 1271 (D. Kan. 2007).....	12
<i>United States v. Monclavo-Cruz</i> , 662 F.2d 1285 (9th Cir. 1981) .....	14
<i>United States v. Park</i> , No. CR 05-375 SI, 2007 U.S. Dist. LEXIS 40596 (N.D. Cal. May 23, 2007) .....	15, 16
<i>United States v. Rabinowitz</i> , 339 U.S. 56 (1950).....	9
<i>United States v. Robinson</i> , 414 U.S. 218 (1973).....	12, 13, 14

<i>United States v. Young</i> , 278 F. Appx. 242 (4th Cir. 2008).....	12
<i>United States v. Zavala</i> , 541 F.3d 562 (5th Cir. 2008).....	4

## **STATUTES**

18 U.S.C. § 2703.....	18
-----------------------	----

## **RULES**

<i>Ohm, Paul Massive Hard Drives, General Warrants, and the Power of Magistrate Judges</i> , 97 VA. L. REV. 1 (2011).....	6
---	---

## STATEMENT OF AMICUS CURIAE

The Electronic Frontier Foundation (“EFF”) is a non-profit, member-supported civil liberties organization that works to protect rights in the digital world. EFF challenges industry, government and the courts to support free expression, privacy, and openness in the information society.

EFF’s interest in this case arises from its ongoing efforts to encourage the government and the courts to recognize the threats that new technologies pose to civil liberties and personal privacy. EFF has special familiarity with and interest in constitutional privacy issues that arise with new technologies, and has served as *amicus* in recent key Fourth Amendment cases including *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) and *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

EFF believes that warrantless searches of electronic storage devices threaten to render meaningless the Fourth Amendment’s prohibition against unreasonable search and seizure. In this case, the Court will decide the extent to which constitutional protections extend to sensitive data stored on cell phones in the context of the search-incident-to-arrest exception to the Fourth Amendment of the United States Constitution and Article I, Section 9 of the Oregon Constitution. We urge the Court to define an important limit to the government’s authority to collect digital information about its citizens

and hold that law enforcement officers must have a warrant supported by probable cause to search a portable digital device seized upon arrest.

### **SUMMARY OF ARGUMENT**

A cell phone is small enough to slip into a pocket, but holds an exhaustive record of its owner's day-to-day existence. Portable digital devices contain a tremendous amount of personal information about users and their activities. This Court should hold that the search-incident-to-arrest exception to the Fourth Amendment does not justify the warrantless search of a digital device seized upon arrest. The United States Supreme Court has long held that purpose for the exception is rooted in exigency: the need for officer protection and the need to ensure that the arrestee cannot destroy evidence. Neither basis applies where the police seize a cell phone from an arrestee and search it only later, when it is under the exclusive control of the police. This Court should require the police to obtain a warrant to search a cell phone under these circumstances.

### **ARGUMENT**

The Fourth Amendment to the United States Constitution protects people against unreasonable searches and seizures, requiring law enforcement officers to obtain a warrant based on probable cause subject to only a few narrow exceptions. *Katz v. United States*, 389 U.S. 347, 357

(1967). In this case, the Court will determine whether the search-incident-to-arrest exception allows police officers to peruse the full contents of a person's cell phone merely because that person has been arrested. The answer is no.

The search-incident-to-arrest exception does not give police free rein to sort through an arrestee's private information for investigatory purposes. The exception is intended to provide safety to law enforcement and bystanders and to prevent the destruction and concealment of evidence. *Chimel v. California*, 395 U.S 752 (1969). Applying the exception to the contents of cell phones does not serve those purposes, and is highly intrusive because of the nature and scope of information that people keep on those devices. And the rule that the Court adopts in this case will likely have consequences that extend beyond cell phones to other digital devices that individuals carry everyday, such as laptops.

If the search-incident-to-arrest exception allows the police to search a digital device after its owner is taken into custody and no longer has control over it, officers will have incentive to search all arrestees' devices as a routine matter rather than seek a probable cause warrant later that might be limited in scope. *See United States v. Comprehensive Drug Testing*, 621 F.3d 1168, 1178-80 (9th Cir. 2010) (Kozinski, J., concurring) (offering

guidance to help magistrate judges ensure that warrants for digital searches do not become general warrants). This Court should not let the search-incident-to-arrest exception swallow the Fourth Amendment rule.

**I. People Have A Strong Expectation Of Privacy In The Information Stored On Their Cell Phones And Other Portable Digital Devices.**

The touchstone question for any Fourth Amendment inquiry is whether an individual has a reasonable expectation of privacy in the item he seeks to protect. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). A cell phone easily passes this test because it contains a tremendous amount of personal information about the user and his activities. It is not surprising, therefore, that many courts have found that individuals have a reasonable expectation of privacy in the information on their cell phones.<sup>1</sup>

The more basic types of these devices typically contain an address book full of information about the user's friends, family and colleagues; a log of calls to or from these people; and text messages to or from them. The phone may be used to access voicemail stored by the service provider. If the phone has a camera, the device likely contains photos snapped by the user.

---

<sup>1</sup> See, e.g., *Ohio v. Smith*, 920 N.E.2d 949, 955 (Oh. 2009), *reconsideration denied*, 921 N.E. 2d 248, *cert. denied*, 131 S. Ct. 102 (2010); *United States v. Zavala*, 541 F.3d 562, 577 (5th Cir. 2008); *United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007); *Connecticut v. Boyd*, 992 A.2d 1071, 1081 n.9 (Conn. 2009) (cataloging cases in which courts have found a reasonable expectation of privacy in information stored on a cell phone).

And the more sophisticated smartphones offer greater computing power, more features and Internet connectivity.<sup>2</sup> Such devices may hold a detailed accounting of the user's Internet browsing history, which reflects personal interests and beliefs.

Many people carry these devices on a daily basis as they go about their lives. In past eras individuals would have kept most or all of their personal papers or sensitive information in their homes, where it would enjoy the strongest Fourth Amendment protection. But the vast majority of people around the globe now own cell phones,<sup>3</sup> and Americans are increasingly abandoning traditional modes of voice communication for more sophisticated mobile devices.<sup>4</sup> According to a 2010 study by Nielsen, most cell phone users will own smartphones by the end of this year.<sup>5</sup> Today,

---

<sup>2</sup> See generally Wikipedia's entry for "Smartphone" at <https://secure.wikimedia.org/wikipedia/en/wiki/Smartphone> (last visited March 30, 2011).

<sup>3</sup> Associated Press, *Number of Cell Phones Worldwide Hits 4.6B*, <https://www.cbsnews.com/stories/2010/02/15/business/main6209772.shtml> (Feb. 15, 2010).

<sup>4</sup> See Associated Press, *1 in 4 Homes Have Cell Phone, No Landline*, CBS News, <https://www.cbsnews.com/stories/2010/05/12/tech/main6476743.shtml> (May 12, 2010).

<sup>5</sup> Roger Entner, *Smartphones to Overtake Feature Phones in U.S. by 2011*, Nielsen Wire, <https://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011> (March 26, 2010); Kevin C. Tofel, *1 in 2 Americans Will Have a Smartphone by Christmas 2011*, Gigaom, <https://gigaom.com/2010/03/26/1-in-2-americans-will-have-a-smartphone-by-christmas-2011> (March 26, 2010).

many people keep cell phones, laptops, iPads, and other portable electronic storage devices within arm's reach at all times.

Digital devices have increasingly large information storage capacities, the vastness of which defies any real-world analogy. *See, i.e.*, Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. 1, 5-8 (2011) (discussing how hard drives of folders and documents are very different than filing cabinets — or even warehouses — of folders and documents). If an individual filled a pick-up truck with books, the amount of text he hauled could be stored in a single gigabyte of electronic storage;<sup>6</sup> the Apple iPhone 4 — one of the most popular smartphones on the market — can carry as much as 32 gigabytes.<sup>7</sup> According to one estimate, 32 gigabytes can hold more than 640,000 Microsoft Word .doc pages, 19,200 photographs, or 2,048 MP3 audio files.<sup>8</sup>

Laptops are just as portable as cell phones and have even greater storage capacity. One of Amazon.com's current best-selling laptops is the

---

<sup>6</sup> Peter Lyman and Hal R. Varian, University of California Berkeley School of Information, *How Much Information? 2003*, <https://www2.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm> (Oct. 23, 2003).

<sup>7</sup> Apple, *iPhone 4 Technical Specifications*, <https://www.apple.com/iphone/specs.html> (last visited March 27, 2011).

<sup>8</sup> CFGear, *How much data can a USB flash drive hold?*, <https://www.cfgear.com/how-much-data-can-a-usb-flash-drive-hold> (April 5, 2010).

15.6-inch Toshiba Satellite L655, which comes with 640 GB of storage capacity in its hard drive.<sup>9</sup> That means that it can hold more text than six floors of an academic research library.<sup>10</sup> And the amount of storage in computers will continue to increase by exponential proportions every year.<sup>11</sup>

Many portable digital devices can wirelessly connect to the Internet, which makes it possible to access data stored far beyond the device itself. This is possible because mobile phones contain usernames, passwords and other credentials that identify, authenticate, and authorize people to access a broad range of services — often automatically, allowing anyone with possession of the device to access the information stored elsewhere.

For example, an individual may use credentials stored on a cell phone to access email stored on her employer's computers or with companies such as Google or Yahoo.<sup>12</sup> Users can also use credentials to access their accounts on social networking services like Facebook, Twitter and MySpace

---

<sup>9</sup> Amazon, *Bestselling in Laptop Computers*, <https://www.amazon.com/gp/bestsellers/pc/565108> (last visited March 27, 2011), *Toshiba Satellite L655-S5158 15.6 Inch Laptop (Black): Computer & Accessories*, <https://www.amazon.com/Toshiba-Satellite-L655-S5158-15-6-Inch-Laptop/dp/B004GHNQDQ>, (last visited March 27, 2011).

<sup>10</sup> Lyman and Varian, *How Much Information?*, *supra* at note 6.

<sup>11</sup> See “Kryder’s Law,” Wikipedia, [https://secure.wikimedia.org/wikipedia/en/wiki/Mark\\_Kryder](https://secure.wikimedia.org/wikipedia/en/wiki/Mark_Kryder) (last visited March 27, 2011); see also Chip Walter, *Kryder’s Law*, SCIENTIFIC AMERICAN, <https://www.scientificamerican.com/article.cfm?id=kryders-law> (Aug. 2005).

<sup>12</sup> See <https://www.google.com> and <https://www.yahoo.com>.

through their mobile devices.<sup>13</sup> Furthermore, services such as Google Docs, Dropbox, and Box.net offer gigabytes of storage to allow users to have the same information on different computers and devices, as well as back up and store files on the Internet.<sup>14</sup>

In sum, people store and access tremendous amounts of private information on the electronic devices they carry with them every day. If the court accepts the government's position, a person's digital life will be an open book for law enforcement whenever the owner of a device is arrested.

## **II. The Search-Incident-To-Arrest Doctrine Does Not Legitimize The Warrantless Search Of The Entire Contents Of A Cell Phone.**

Once a digital device is securely in police hands, there is no danger to the arresting officers, no possibility of destroying evidence, and “no possibility that an arrestee could reach into the area that law enforcement officers seek to search.” *Arizona v. Gant*, \_\_\_ U.S. \_\_\_, 129 S. Ct. 1710, 1716 (2009). The search-incident-to-arrest exception should not apply under these circumstances. Allowing otherwise would be tantamount to “giving police officers unbridled discretion to rummage at will among a person's private

---

<sup>13</sup> See <https://www.facebook.com>, <https://www.twitter.com>, and <https://www.myspace.com>.

<sup>14</sup> See <https://docs.google.com>, <https://www.dropbox.com>, and <https://box.net>. These “cloud” storage services are popular. For example, according to Dropbox's website, the service has “millions of users.” *About Dropbox*, <https://www.dropbox.com/about> (last visited March 27, 2011).

effects,” *Gant*, 129 S. Ct. at 1720, or permitting officers to rifle through the desk drawers in a room where one is arrested, *Chimel*, 395 U.S. at 763, propositions explicitly rejected by this nation’s highest court.

**A. The Search-Incident-To-Arrest Exception Does Not Apply Where Officer Safety, Evidence Destruction Or Other Exigencies Are Not Concerns.**

The Supreme Court has long held that purpose for the search-incident-to-arrest exception is rooted in exigency: most notably, the need for officer protection and the need to ensure that evidence is not destroyed by the arrestee. *Gant*, 129 S. Ct. at 1714; *Chimel*, 395 U.S. at 753; *see also United States v. Rabinowitz*, 339 U.S. 56, 72 (1950) (Frankfurter, J., dissenting) (discussing the history of the search-incident-to-arrest exception). But such searches “must not be a ruse for a general rummaging in order to discover incriminating evidence.” *United States v. Feldman*, 788 F.2d 544, 553 (9th Cir. 1986).

The Court emphasized this principle just two years ago when it struck down the warrantless search of an arrestee’s jacket pocket inside a car after he was in custody and no longer able to access the interior of his vehicle. In *Arizona v. Gant*, the police arrested the defendant for driving with a suspended license. 129 S. Ct. at 1714. While he was in custody and handcuffed in the back of a patrol vehicle, the officers searched the inside of his car without a warrant and found cocaine in the pocket of a jacket on the

backseat. *Id.* The Court explained: “If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and *the rule does not apply.*” *Id.* at 1716 (emphasis added). The Court further elaborated:

A rule that gives police the power to conduct [a search incident to arrest] whenever an individual is caught committing a traffic offense, when there is no basis for believing that evidence of the offense might be found in the vehicle, creates a serious and reoccurring threat to the privacy of countless individuals. Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment — the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.

*Id.* at 1720.

The Court’s reasoning in *Gant* flows logically from *Chimel v. California*, a case in which police officers searched the defendant’s entire home incident to a lawful arrest. 395 U.S. 752, 753 (1969). The Court found the search unconstitutional, determining that the police may search an area incident to arrest only if the space is within an arrestee’s “immediate control” — specifically, “the area from within which he might gain possession of a weapon or destructible evidence.” *Id.* at 763. The Court noted that the rule “grows out of the inherent necessities of the situation at the time of arrest.” *Id.* at 759 (quoting *Trupiano v. United States*, 334 U.S. 699, 705, 708 (1948)). The Court concluded, however, that there is no

justification “for routinely searching any room other than that in which an arrest occurs — or, for that matter, for searching through all the desk drawers or other closed or concealed areas in that room itself.” *Chimel*, 395 U.S. at 763.

*Gant* is also consistent with *United States v. Chadwick*, 433 U.S. 1 (1977), *abrogated on other grounds*, *California v. Acevedo*, 500 U.S. 565 (1982). In that case, federal officers arrested the defendants and seized from their car trunk a locked footlocker, which the officers had probable cause to believe contained drugs. *Chadwick*, 433 U.S. at 4. Approximately an hour and a half after the arrest, the agents opened and searched the footlocker without a warrant while the defendants were in custody and the officers had exclusive control over the container. *Id.* at 4-5. The Supreme Court found the search unconstitutional, explaining:

Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.

*Id.* at 15.

Some courts have relied on the Supreme Court’s holdings in *United States v. Robinson*, 414 U.S. 218 (1973) and *United States v. Edwards*, 415 U.S. 800 (1974) to hold that officers can search arrestees’ cell phones

incident to arrest, concluding that they are part of the arrestee's "person." See, e.g., *People v. Diaz*, 244 P.3d 501 (Cal. 2011); *United States v. Finley*, 477 F.3d 250 (5th Cir. 2007); *United States v. Young*, 278 F. Appx. 242 (4th Cir. 2008); *United States v. Mercado-Nava*, 486 F. Supp. 2d 1271 (D. Kan. 2007).<sup>15</sup> *Robinson* and *Edwards*, decided nearly 30 years ago, should be read narrowly in light of the more recent holdings in *Chadwick* and *Gant*. Searches of the person are distinguishable from searches of electronic data stored in devices carried by the person, making *Chadwick* and *Gant* more directly applicable.

In *Robinson*, the police pulled over the defendant because they believed that he was driving with a revoked permit and placed him under arrest. 414 U.S. 218 at 220. While the defendant was in custody, an officer searched him and discovered a crumpled cigarette package in his coat pocket with heroin inside. *Id.* at 222-23. The Supreme Court upheld the warrantless search, explaining that the search-incident-to-arrest exception "has historically been formulated into two distinct propositions. The first is that a search may be made of the *person of the arrestee* by virtue of the lawful arrest. The second is that a search may be made of the *area within*

---

<sup>15</sup> Indeed, many of these cases were decided before *Gant* reaffirmed that the exception does not apply "where there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search." 129 S. Ct. at 1716.

*the control of the arrestee.*” *Id.* at 224 (emphasis added). The Court concluded that the police searched and seized the package during a lawful custodial search of the defendant’s person. *Id.* at 236.

In *Edwards*, the defendant was arrested and taken into custody for trying to break into a post office. 415 U.S. at 801. The police investigating the scene noticed that a window had been pried open and that there were paint chips on the windowsill and screen. *Id.* at 801-02. The police seized the defendant’s clothes without a warrant the next morning while he was still in custody and examined them for evidence, discovering paint chips that matched those found at the window. *Id.* at 802. The Court upheld the search under the search-incident-to-arrest exception, reasoning that the police had probable cause to believe that the clothes themselves were evidence of the crime for which the defendant was arrested. *Id.* at 804-05. The Court was careful to reserve the possibility that a warrant might be required for officers to search “the effects” of an arrestee under other circumstances. *Id.* at 808.

The cell phone in this case is more like the footlocker in *Chadwick* and the jacket pocket in *Gant* than the cigarette package in *Robinson* or the clothing worn by the defendant in *Edwards*. In the former cases, the searched item was a possession in the exclusive control of the police, raising

no concerns about officer safety or destruction of evidence. In *Robinson* and *Edwards*, the searches upheld by the Supreme Court were of the arrestee's person, and did not involve a closed possession in the hands of the police. While an arrestee may have a reduced privacy interest in his person, he does not have a reduced privacy interest in the contents of his phone in police custody.

The Ninth Circuit explained this distinction effectively in *United States v. Monclavo-Cruz*, in which the police searched the defendant's purse without a warrant at the station house an hour after her arrest. 662 F.2d 1285 (9th Cir. 1981). The court interpreted the holdings in *Chadwick*, *Edwards* and *Robinson* to mean that "once a person is lawfully seized and placed under arrest, she has a reduced expectation of privacy in her person," while "possessions within an arrestee's immediate control have [F]ourth [A]mendment protection at the station house *unless the possession can be characterized as an element of clothing.*" *Id.* at 1290 (emphasis added). While the cigarette package in *Robinson* was closely enough associated with clothing to fall within the exception, a purse seized from the defendant was not. *Id.* Likewise, a cell phone — with its tremendous capacity for storage and high likelihood of carrying vast amounts of information — is a possessory item in which a person retains a strong privacy interest, and

cannot simply be considered “an element of clothing.”

The outcome of this case should be similar to *United States v. Park*, in which law enforcement officers used the search-incident-to-arrest doctrine to search several suspects’ cell phones for telephone numbers during the booking process approximately an hour and a half after the suspects’ arrests. No. CR 05-375 SI, 2007 U.S. Dist. LEXIS 40596, at \*\*5-13 (N.D. Cal. May 23, 2007). The court held that the government did not meet its burden to establish that an exception to the warrant requirement applied to justify the searches. *Id.* at \*14. Specifically, it found that cell phones should be considered “possessions within an arrestee’s immediate control” — in which an arrestee has no reduced expectation of privacy and which receive full Fourth Amendment protection at the police station — rather than part of “the person,” an area in which there is a reduced expectation of privacy after arrest. *Id.* at \*21, citing *Chadwick*, 433 U.S. at 16 n.10. Critical to the court’s decision was the fact that “[i]ndividuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.” *Id.* at \*22. Furthermore, the court noted that the searches went “far beyond the original rationales for searches incident to arrest, which were to remove weapons to ensure the safety of officers and

bystanders, and the need to prevent concealment or destruction of evidence.”

*Id.* at \*24. *Cf. Smith*, 920 N.E.2d at 955.

Like the defendants in *Park*, the defendant in this case was in police custody when officers searched his cell phone approximately 40 minutes after arrest. ER-3. At the time of the search, the defendant was in a holding cell and posed no danger to any member of law enforcement, nor any threat of destroying evidence. ER-3. A police crime analyst accessed the defendant’s cell phone solely to search for evidence, and in fact found text messages and images that he believed were related to this purpose. ER-3-4. Like the search in *Park*, the warrantless search of the defendant’s cell phone here was a fishing expedition for incriminating evidence, and had nothing to do with preserving evidence or protecting officer safety. The search was unconstitutional.

**B. No Exigency Exists To Justify The Routine Warrantless Search Of Cell Phones Incident To Arrest.**

The only potential exigency raised by the officers to justify the search-incident-to-arrest exception here is the possible loss of evidence if they are required to obtain a warrant. This is not a compelling argument.

While programs exist that allow a user to remotely delete the data on a

device,<sup>16</sup> these programs cannot delete data unless the user takes an affirmative action to trigger the deletion, typically by signing into an account online and indicating that he wishes to “wipe” the data on the device — something difficult to accomplish while in custody. It is also unlikely that an arrestee could erase the data on a device by placing a collect call to a service provider from a detention room, as the trial court noted. ER-5-6.

Regardless, any concern about remote wiping can be eliminated by placing the seized device in a container that keeps the phone from receiving outside communications and maintains the integrity of the data on the device for evidentiary purposes.<sup>17</sup> Immediately upon arrest, officers can deposit cell phones and other digital devices into bags that serve this purpose.<sup>18</sup> To the extent that officers are concerned that the device’s battery may run out before they can secure a warrant, they can charge the battery using a power adapter that plugs into the wall or a car, or a remote charger.

---

<sup>16</sup> See Jamie Lendino, *Kill Your Phone Remotely*, PCMag.com, <https://www.pcmag.com/article2/0,2817,2352755,00.asp> (Sept. 11, 2009) (surveying the remote wiping software available for different mobile phones).

<sup>17</sup> See “Faraday cage,” Wikipedia, [https://secure.wikimedia.org/wikipedia/en/wiki/Faraday\\_cage](https://secure.wikimedia.org/wikipedia/en/wiki/Faraday_cage) (last visited March 30, 2011).

<sup>18</sup> See, e.g., Paraben Corporation, Patented Wireless StrongHold Bag, <https://www.paraben.com/stronghold-bag.html> (last visited March 28, 2011); Disklabs, The Mobile Phone Shield Faraday Bag, [https://www.faradaybag.com/faraday\\_bag\\_mobile\\_shield.html](https://www.faradaybag.com/faraday_bag_mobile_shield.html) (last visited March 28, 2011); eDEC, RF Shielded Bags for Forensically Sound Evidence Collection, <https://www.faraday-bags.com> (last visited March 28, 2011).

Officers can also seek records of the device's communications from the communications service provider that the arrestee subscribes to, such as AT&T or Verizon. *See United States v. James*, No. 1:06CR134 CDP, 2008 U.S. Dist. LEXIS 34864 at \*19 n.3 (E.D. Mo. April 29, 2008). If officers can satisfy the appropriate legal standard, they can obtain various records from providers through a warrant, subpoena, or court order. *See, i.e.*, Stored Communications Act, 18 U.S.C. § 2703.

It is doubtlessly true that it is more inconvenient for the police to have to obtain a warrant before searching a digital device. But inconvenience does not justify a warrantless search of all cell phones upon arrest: “the Constitution recognizes higher values than speed and efficiency.” *Stanley v. Illinois*, 405 U.S. 645, 656 (1972); see also *United States v. Karo*, 468 U.S. 705, 717-18 (1984) (rejecting argument that a warrant requirement should not apply because officers will be forced to obtain warrants in more situations). Refusing to apply the search-incident-to-arrest exception here will not hamstring the government's ability to investigate crimes. It will simply require agents to obtain a probable cause warrant to search a digital device for evidence after an arrestee is taken into custody, consistent with *Gant* and *Chadwick*.

**CONCLUSION**

For the foregoing reasons, the Court should find that the search-incident-to-arrest exception does not apply and the search of the defendant's cell phone violated the Fourth Amendment.

Dated: April 1, 2011

Respectfully submitted,

*/s/ Marcia Hofmann*

Marcia Hofmann, CA Bar No. 250087  
Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, CA 94110  
(415) 436-9333  
(415) 436-9993 (fax)

J. Ashlee Albies  
OR Bar No. 05184  
Creighton & Rose, PC  
815 SW Second Ave., Suite 500  
Portland, OR 97204  
(503)221-1792  
(503) 223-1516

Attorneys for *Amicus Curiae*

## CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Oregon Rule of Appellate Procedure 5.05(b)(ii) because this brief contains 4,191 words, excluding the parts of the brief exempted by Oregon Rule of Appellate Procedure 5.05(2)(a).

2. This brief complies with the typeface and type style requirements of Oregon Rule of Appellate Procedure 5.05(d)(2) because this brief has been prepared in a proportionally spaced Times New Roman typeface, 14-point font.

Dated: April 1, 2011

Respectfully submitted,

*/s/ J. Ashlee Albies*

J. Ashlee Albies  
OR Bar No. 05184  
Creighton & Rose, PC  
815 SW Second Ave, Suite 500  
Portland, OR 97204

*Attorney for Amicus Curiae*

**CERTIFICATE OF SERVICE  
NOTICE OF FILING AND PROOF OF SERVICE**

I certify that I directed the original *amicus curiae* brief to be filed with the Appellate Court Administrator, Appellate Courts Records Section, 1163 State Street, Salem, Oregon, 97301, on April 1, 2011, by electronic filing.

I further certify that a copy of the *amicus curiae* brief was e-served pursuant to ORAP 16.45 on Bronson D. James (#033499), attorney for the Petitioner, on April 1, 2011.

I further certify that a copy of the *amicus curiae* brief was e-served pursuant to ORAP 16.45 on John R. Kroger (#077207), Mary H. Williams (#911241), and Douglas Zier (#804174), attorneys for the Respondent, on April 1, 2011.

Dated: April 1, 2011

Respectfully submitted,

*/s/ J. Ashlee Albies*

J. Ashlee Albies  
OR Bar No. 05184  
Creighton & Rose, PC  
815 SW Second Ave, Suite 500  
Portland, OR 97204

*Attorney for Amicus Curiae*