No. 13-132

IN THE

Supreme Court of the United States

DAVID LEON RILEY,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

On Writ of Certiorari
to the California Court of Appeal,
Fourth Appellate District

REPLY BRIEF FOR PETITIONER

Patrick Morgan Ford
LAW OFFICE OF PATRICK MORGAN FORD
1901 First Avenue
Suite 400
San Diego, CA 92101

Donald B. Ayer
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001

Jeffrey L. Fisher
Counsel of Record
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@law.stanford.edu

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

REPLY BRIEF FOR PETITIONER

The State maintains that anytime a police officer arrests a person for any offense, the police department should be automatically entitled to conduct an unbounded, warrantless search of the person's smartphone. According to the State, precedent commands such a wide-ranging and absolute authority, and it is necessary to serve various law enforcement interests.

But this Court's holding in *United States v. Robinson*, 414 U.S. 218 (1973), does not mandate the categorical ruling the State seeks. That decision was issued before the advent of smartphones – devices increasingly necessary to navigate innumerable tasks of daily life and on which people now carry the entirety of their private papers in their pockets or purses. Nor do any of the law enforcement interests the State identifies support the rule it seeks. These interests merely show that in certain isolated situations, exigent circumstances may justify inspecting smartphones before warrants could reasonably be obtained.

That leaves the State's and the United States' attempts to mitigate the dramatic implications of the power they seek. The State's suggestion that this Court simply leave it to legislatures, police officers, or future cases to limit the scope of smartphone searches is unconvincing. And the United States' various fallback positions either fail to meaningfully curb the authority it requests or would be entirely unworkable. The decision below should be reversed.

I. The Fourth Amendment Prohibits Searching The Digital Contents Of Smartphones Incident To Arrest.

A. *Robinson* Does Not Confer A Categorical Authority To Search Smartphones.

The State argues that when the police seize a smartphone from an arrestee's person, this Court's holding in *United States v. Robinson*, 414 U.S. 218 (1973), mandates that officers have a categorical right – irrespective of the factors outlined in *Chimel v. California*, 395 U.S. 752 (1969) – to explore the smartphone's digital contents. Resp. Br. 10-11. This argument overreads *Robinson.*

1. In *Robinson*, this Court explained that, just like the authority to search an arrestee's grab area, the authority to search an arrestee's person is "based upon the need to disarm and to discover evidence." 414 U.S. at 235; *see also id.* (*Chimel* justifications are "the reasons supporting the authority for a search of the person incident to a lawful arrest"). Subsequent cases say the same. *See, e.g.*, *Virginia v. Moore*, 553 U.S. 164, 176 (2008) (officers may search arrestee's person "in order to ensure their safety and safeguard evidence"); *Knowles v. Iowa*, 525 U.S. 113, 118 (1998) (same).

Robinson simply held that when it comes to purely physical items on an arrestee's person, one or both of the *Chimel* justifications is so likely, if not inherently, present that case-by-case adjudication is unwarranted. *See Robinson*, 414 U.S. at 235; *see also Chimel*, 395 U.S. at 763 (same with respect to grab area). *Robinson* did not consider – nor could it have –

whether the same reasoning applies to digital data on a smartphone.

2. The State responds that *Robinson* nevertheless confers the categorical authority it seeks because this Court's opinion notes that when an item is seized from an arrestee's person, "the mere fact of a lawful custodial arrest" reduces an arrestee's expectation of privacy in the item. Resp. Br. 25; *see also* U.S. Br. 8-9 (stressing same point).[1] But nothing about this reality creates a categorical power, untethered from *Chimel*, to search smartphones.

a. While an arrest diminishes an arrestee's expectation of privacy in his person, "the mere fact of a lawful arrest does *not* end our inquiry." *Schmerber v. California*, 384 U.S. 757, 769 (1966) (emphasis added). That is, not every search of an arrestee's personal effects "is acceptable solely because a person is in custody." *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013). Such searches "must [still] be tested by the Fourth Amendment's general proscription against unreasonable searches." *United States v. Edwards*, 415 U.S. 800, 808 n.9 (1974). Accordingly, when searching an arrestee involves categorically "greater intrusions or higher expectations of privacy," then the privacy-related concerns may be "weighty enough that the search may require a warrant." *King*, 133 S. Ct. at 1979.

Indeed, for just these reasons, the Court has long deemed the authority described in *Robinson* inapplicable to one type of search of an arrestee's

---

[1] Unless otherwise noted, references are to the United States' brief in this case, not *United States v. Wurie*, No. 13-212.

person. Notwithstanding the language in historical materials describing an "unrestricted" right to search the persons of arrestees, this Court has held that when police wish to search beneath the body's surface, Fourth Amendment privacy interests require the police, absent exigent circumstances, to seek a warrant. *Schmerber*, 384 U.S. at 769-70; *see also Missouri v. McNeely*, 133 S. Ct. 1552, 1564, 1559 n.3 (2013) (recognizing that *Robinson* is inapplicable in the context of drawing blood incident to arrest). The question here, therefore, is not whether this Court should create an exception to some preexisting, absolute authority to search the persons of arrestees, but rather – as in *Schmerber* – whether it is reasonable to extend the authority described in *Robinson* to a new kind of search that prior generations could never have envisioned.

b. It would be unreasonable to render the mere fact of an arrest sufficient cause for police to conduct a warrantless, exploratory search of an arrestee's smartphone. A smartphone holds exponentially greater amounts of sensitive information than any physical item an arrestee could carry on his person. Smartphones accordingly implicate the Fourth Amendment's core prohibition against general warrants in a way that searching physical items cannot. *See* Petr. Br. 29.

The State resists this analogy, protesting that digital information on smartphones – while admittedly more voluminous – "is not different in kind from what the law has [allowed to be searched incident to arrest] for many years." Resp. Br. 9, 46; *see also* U.S. Br. 22 (same argument). This argument bears a striking resemblance to the position the

Government unsuccessfully advanced in *United States v. Jones*, 132 S. Ct. 945 (2012). It is even less persuasive here.

In *Jones*, the United States marshaled two cases, *United States v. Karo*, 468 U.S. 705 (1984) and *United States v. Knotts*, 460 U.S. 276 (1983), purportedly establishing a categorical rule that people lack any reasonable expectation of privacy in movements through public areas. The Government then argued that "although GPS technology is more advanced than the beeper technology" used in those cases, this technological advance was irrelevant because "it reveals the same type of information" as beepers do. U.S. Reply Br. 1, *United States v. Jones*, 132 S. Ct. 945 (2012) (No. 10-1259). Not one Justice agreed with this argument, and five squarely rejected it. As Justice Alito explained, the "practical" capability of GPS technology to aggregate information in a manner unforeseeable to prior generations rendered the privacy implications different not just in degree but in kind. *Jones*, 132 S. Ct. at 963-64 (concurring in judgment); *see also id.* at 956 (Sotomayor, J., concurring).

So too here. Searching a smartphone is different in kind than searching any purely physical object that might be seized from an arrestee – even something like a wallet or spiral notebook. As numerous *amici* elaborate, smartphones contain truly massive quantities of information – "the equivalent of [carrying in one's pocket] the cabinets, desks, bookshelves, and bureaus in an eighteenth century home," Br. of ACLU 6, as well as one's entire office, library, *see* Br. of Am. Library Ass'n 13-15, random thoughts and wonders, and collections of medical,

financial, and consumer records. *See also* Br. of NACDL 3-6. Furthermore, smartphones contain not merely more information, but new types of information (such as GPS-locational information and real-time physiological data) different from anything a person carried in the days of purely analog belongings.[2] With each passing year, the smartphone will only become more of a nerve center for our daily activities, relationships, and very identities. *See, e.g.*, Erik Brynjolfsson & Andrew McAfee, The Second Machine Age 34 (2014); Eric Schmidt & Jared Cohen, The New Digital Age 13-59 (2013).

Contrary to the State's insistence (Resp. Br. 47-50), the expressive nature of the virtual warehouses of information on smartphones only accentuates the privacy stakes involved. The State cites several old cases supposedly establishing a historical indifference to searching private papers incident to arrest. But the State's cases establish merely that officers could historically seize papers, just like non-expressive items, when they were "instruments" of the crime of arrest. *Gouled v. United States,* 255 U.S. 298, 309-10 (1921); *see also Marron v. United States*, 275 U.S. 192, 199 (1927) (papers were

---

[2] For example, Samsung's latest phones contain heart-rate monitors. Smartphone apps can sync with Fitbits – small monitoring devices worn on the wrist – to collect and store a user's sleep patterns and calories burned. *See Fitbit*, http://www.fitbit.com/flex. Smartphones will also soon be used to "keep track of your blood pressure, detect nascent heart disease[,] identify early-stage cancer" and "monitor [] insulin levels." Eric Schmidt & Jared Cohen, The New Digital Age 25 (2013).

"actually used to commit the offense"); *Dillon v. O'Brien & Davis*, 16 Cox C.C. 245, 247 (Exch. Div. Ir. 1887) (papers were "being used for the purpose of such combination and conspiracy"). Indeed, in *United States v. Kirschenblatt*, 16 F.2d 202 (2d Cir. 1926) – the very case the United States quotes for the supposedly absolute principle that "the law has never distinguished between documents and other property found upon the person of one arrested" – Judge Hand stressed that seizing a few papers that are instrumentalities of crime is fundamentally different from "rummag[ing] at will among [an arrestee's] papers in search of whatever will convict him." *Id.* at 203, quoted in U.S. Br. 6, 26. Allowing the latter – he believed and other historical sources demonstrate – would "countenance exactly what the amendment was designed to prevent." *Id.* at 204; *see also* Petr. Br. 31-32, 34-36.

c. Finally, distinguishing as sharply as the State would between smartphones seized from a person's pocket and phones seized from an arrestee's immediate vicinity would be irrational. This Court has stressed that Fourth Amendment rules "must not turn on . . . coincidences" or mere happenstance. *California v. Acevedo*, 500 U.S. 565, 580 (1991). Partly for this reason, *Chimel* itself emphasized that searches of persons and the area into which an arrestee might reach "must, of course, be governed by a like rule." 395 U.S. at 763. Given that a smartphone is just as likely to be in an arrestee's pocket as sitting nearby in her briefcase or on her desk, such an extraordinary privacy interest should not be dependent on whether the arrestee is holding the phone at the moment of apprehension or whether it is sitting inches away.

B. No Governmental Interest Requires A Categorical Authority To Search Smartphones Incident To Arrest.

None of the State's arguments about officer safety, destruction of evidence, or identifying arrestees satisfies *Chimel*'s standard for allowing categorical warrantless searches incident to arrest. At the very most, the State imagines a few isolated scenarios that would trigger the exigent circumstances doctrine.

1. Officer Safety

a. *Bombs.* The State posits that smartphones can be used as (or to trigger) bombs. Resp. Br. 30. This scarcely resonates as an everyday concern. If ever it does arise, this Court has already held that "if officers have reason to believe that [a seized item] contains some immediately dangerous instrumentality, such as explosives," the exigent circumstances doctrine allows officers to search it immediately. *United States v. Chadwick*, 433 U.S. 1, 15 n.9 (1977). The State offers no reason why the same would not be true here.

b. *Confederates.* The State also hypothesizes that arrestees might use smartphones "to summon assistance from confederates." Resp. Br. 30. But even though cell phones have been in widespread use for over a decade, the State fails to cite a single instance, over tens of millions of arrests, in which one has ever been used to do this. Crediting a possibility so "remote in the extreme" to allow blanket authority for searches incident to arrest would stretch "current doctrine . . . beyond its breaking point." *Thornton v. United States*, 541 U.S. 615, 625 (2004) (Scalia, J., concurring in judgment). As with a possible bomb, if

officers really think that an arrestee may have summoned an ambush, exigent circumstances would permit inspection of the phone.

2. Preserving Evidence

The State also contends that warrantless searches incident to arrest are necessary to prevent digital data from being remotely wiped or rendered forever inaccessible behind personal security features. Once again, neither of these arguments justifies the categorical authority the State seeks.

a. *Remote wiping.* Contrary to the State's contentions, simple steps that officers already take on a daily basis allay any concern that a phone might be remotely wiped.

As an initial matter, it is customary for officers first to put seized smartphones in airplane mode. *See* Rick Ayers et al., National Institute of Standards and Technology, U.S. Dept. of Commerce, Guidelines on Mobile Device Forensics (DRAFT) 36-37 (Sept. 2013) ("NIST Draft Guidelines").[3] The State complains that this "requires officers to interact with the phone." Resp. Br. 38. But triggering airplane mode is much easier than doing something else the State confidently reports that officers can do: search throughout a phone while taking care not to alter or delete any of its contents. It takes only one or two clicks in a phone's settings (regardless of whether it is locked) to put it in airplane mode. *See* Appendix A. And while the State muses that airplane mode "may

---

[3] http://nist.gov/forensics/research/upload/draft-guidelines-on-mobile-device-forensics.pdf.

not block *all* signals," Resp. Br. 38 (emphasis added), it does completely block remote wiping commands. *See* NIST Draft Guidelines 30.

If for some reason an officer is unable or unwilling to put a phone in airplane mode, Faraday bags are "simple and inexpensive security techniques" that also block remote wiping commands. Br. of EPIC 5. The State responds that Faraday bags may not work forever because they "depend on current technology." Resp. Br. 37. But all smartphones for the foreseeable future will operate via radio waves, and those are what Faraday bags block. If an entirely new basis for smartphone technology someday emerges, this Court could then "revisit this issue." *See United States v. Wurie*, 728 F.3d 1, 13 n.12 (1st Cir. 2013).

The State next notes that Faraday bags "can quickly drain a phone battery." Resp. Br. 39. Yet as any smartphone user can attest, a phone does not lose any perceptible information if its battery dies. This is because smartphones, like other modern computers, keep most everything in permanent storage. The State's suggestion (*id.* at 34) that a phone might lose "content" if its battery dies cites a manual published in 2007, before smartphone technology emerged.[4]

---

[4] The only information the State or United States identifies that might be lost if a *modern* phone's battery dies is an "encryption key." Resp. Br. 40; U.S. Br. 12. But an encryption key matters only if password protection threatens to preclude officers from gaining access to information on a device. For the reasons described in the next subsection, this concern is not at issue here and is highly unlikely to arise in other cases.

Finally, the State argues that Faraday bags "do not reliably block all incoming signals." Resp. Br. 39. It may be true, at least in laboratory settings, that some Faraday bags occasionally let bits of radio waves through. But the proof of the pudding is in the eating: Officers routinely use Faraday bags, *see* Br. of Crim. Law Profs. 4-6, and neither the State nor its *amici* can point to a single instance of a seized phone that was placed in a Faraday bag ever being remotely wiped.[5] Whatever the odds of this occurring someday, they surely pale in comparison to the possibility that "confederates of [a man arrested in his home] will in the meanwhile remove the items for which the police have probable cause to search." *Chimel*, 395 U.S. at 774 (White, J., dissenting). Yet even that potential danger is insufficient to justify warrantless examinations of arrestees' entire homes incident to arrest. *See id.* at 763.

b. *Password protection.* Raising an argument never advanced before the merits briefing in this Court – and, indeed, seemingly never raised previously in *any* appellate proceeding – the State and the United States contend that officers need to "prompt[ly]" search smartphones insofar as passwords might prevent them "at any later time –

---

[5] This reality also disposes of the United States' suggestion that even if a phone is placed in a Faraday bag, any previously blocked remote wiping command could execute as soon as the phone is removed, U.S. Br. 16. Again, the Government offers no evidence of this ever happening. If airplane mode is somehow unavailable and remote wiping is a genuine concern, the police can transport the phone to a signal-proof environment before removing it from the bag.

even with a warrant" from accessing the phones' digital contents. Resp. Br. 33-35; *accord* U.S. Br. 11.

This argument does not apply to the facts of this case. Petitioner's smartphone "was not password-protected." Resp. Br. 52. The photos and videos at issue were stored on a removable memory card which would have been accessible even if the phone had been locked. Petr. Br. 22; *see also, e.g.*, *People v. Blanchette*, 2014 WL 718414, at *2 (Cal. Ct. App. 2014) (describing how police were able to view photos on a password-protected device simply by ejecting the memory card). And the phone was not searched until two hours after its seizure, long after police knew it was not going to lock.[6]

What is more, the State's password-protection argument depends on numerous factual premises that make the concern the State hypothesizes so unlikely to arise that it could not possibly justify the categorical authority the State seeks:

- For starters, the police would have to seize a phone "in an unlocked state." U.S. Br. 13. Yet a phone will not be unlocked unless it has been used within minutes of an arrest. And even then, a user need only press a single button to re-lock the phone. So officers will rarely recover a phone in an unlocked state.

---

[6] The United States suggests that an iPhone's auto-lock feature could suddenly kick in after as much as "four hours." U.S. Br. 11. Not so. The maximum delay is five minutes. *See* Appendix C. The United States references the potential time period before *password protection* kicks in, which does not start running until a phone has already locked.

- If the phone is unlocked, the police would have to be incapable of easily discerning whether the phone is password-protected. Yet an officer need only press a couple of buttons under "settings" to find out whether this is the case. *See* Appendix B.
- If an unlocked phone is indeed password-protected, the police would have to be unable to disable the phone's "auto-lock" feature to prevent the password from kicking in. Yet that too requires pressing only a few buttons. *See* Appendix C.
- The police also would have to want to examine content that is capable of being password-protected. Many phones, including petitioner's and some current Android models, store some or all of their data on memory cards that are accessible regardless of any password-protection.[7]
- The police would have to be unable to ensure future access to the unlocked phone's contents by connecting it to another device, such as a laptop in a police cruiser. Yet according to the NIST Draft Guidelines (at 35), taking this step creates a "trusted relationship" that will "ensure that the data can be accessed at a later time, after the device is locked."
- Lastly, the police would have to be unable to guarantee future access to content on an

---

[7] *See, e.g.*, *Specs*, Samsung Galaxy S5 (2014), http://www.samsung.com/global/microsite/galaxys5/specs.html.

> unlocked phone that is protected by a password simply by asking the owner at the scene for the password. Yet cases demonstrate that this tactic is often successful. *See, e.g.*, *United States v. Williams*, 2014 WL 412526, at *4 (D. Vt. 2014); *United States v. Nyuon*, 2013 WL 1339713, at *3 (D.S.D. 2013); *People v. Villasana*, 2010 WL 7122, at *1 (Cal. Ct. App. 2010); *Newell v. State*, 49 So. 3d 66, 71 (Miss. 2010). Indeed, if refusing to divulge a password could expose one's unlocked phone to a warrantless exploratory search, most individuals presumably would much rather divulge the password for use if the police secure a particularized warrant.

If and when this collection of prerequisites ever comes to pass, then seizing an unlocked phone might give rise to exigent circumstances justifying an immediate warrantless search. *See McNeely*, 133 S. Ct. at 1561. This depends on whether law enforcement is truly at risk of losing access to password-protected content if a smartphone locks without the police having connected it to a trusted source or obtained the password voluntarily from the owner.[8] But whatever the answer to that question,

---

[8] Law enforcement under these circumstances might be able to obtain access to password-protected content in a number of ways. First, the police might be able to require arrestees to turn over their passwords; the United States has argued in the lower courts that an individual lacks any Fifth Amendment right to withhold (or refuse to disable) a password, and some courts have accepted this argument. *See, e.g.*, *United States v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009); *United States v.*

there can be no doubt that the State's speculations fail to establish any categorical need to search *all* smartphones – no matter the circumstances under which they are seized or how long after the seizure they are examined – without a warrant.

3. Identification

Lastly, the State suggests that officers need to search smartphones to identify arrestees. Resp. Br. 31. But the interest in identification relates only to the administrative processing of arrestees. *See King*, 133 S. Ct. at 1971, 1974. This Court has never recognized identification as an independent basis for *searches incident to arrest*. Indeed, when arrestees are apprehended inside their homes, there are no doubt numerous effects close at hand that could identify them – letters, certificates, and personal

---

Fricosu, 841 F. Supp. 2d 1232 (D. Colo. 2012); *contra In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012). If the United States is correct, then law enforcement seemingly has nothing to fear regarding passwords. Second, "some protection mechanisms can be bypassed" in police forensic labs. Resp. Br. 35; *accord* Br. of Ass'n of State Crim. Investigative Agencies et al. 10, 15. Third, cell phone manufacturers appear willing to unlock phones the police are unable to unlock themselves. *See* Cal. Dist. Att'ys Ass'n, Cell Phone Records Training Materials 3753-54, https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_irvine1_irvineca.pdf (providing exemplars for orders to Apple and Google to assist in searching phones by "bypassing the Cell Phone user's passcode"); Declan McCullagh, *How Apple and Google Help Police Bypass iPhone, Android Lock Screens*, CNet (April 2, 2012), http://www.cnet.com/news/how-apple-and-google-help-police-bypass-iphone-android-lock-screens/.

documents – but the Court has never excepted these items from *Chimel*'s limitations on searches.

At any rate, there are far more direct, accurate, and less intrusive methods of identifying arrestees, including looking inside their wallets – not to mention fingerprinting and DNA. *See King*, 133 S. Ct. at 1977.

C. None Of The State's Or The United States' Attempts To Mitigate The Implications Of Their Positions Is Persuasive.

Perhaps recognizing the startling implications of the categorical rule they seek, the State and United States offer various proposals for limiting the impact of a decision in their favor. None succeeds.

1. Contrary to the State's suggestions (Resp. Br. 52-57), this Court cannot simply leave it to others to restrict the scope of smartphone searches. This Court, not legislatures, determines the Fourth Amendment's meaning. In any event, legislatures show no sign of entering this realm. Nor can protecting smartphone privacy be left to officer discretion. The Bill of Rights "protects against the Government; it does not leave us at the mercy of *noblesse oblige*." *United States v. Stevens*, 130 S. Ct. 1557, 1591 (2010). Accordingly, this Court will not uphold an otherwise unconstitutional power "merely because the Government promise[s] to use it responsibly." *Id.*[9]

---

[9] The United States asserts that requiring a warrant would not constrain officer discretion because warrants would merely

Nor can this Court leave problems of scope to future cases. The State urges this Court to hold that examining the photo and video files on petitioner's phone was reasonable because at least those particular digital files "are not fundamentally different from, or more sensitive than, other types of personal information long carried by individuals in non-digital forms." Resp. Br. 43. But this argument ignores the sheer quantities of information that smartphones enable people to carry. *See* Petr. Br. 26-27; Br. of CDT & EFF 7-8. No one can lug around thousands of non-digital photos or videos. Nor would anyone have any customary reason even to try to do so. The pervasiveness of smartphone technology, by contrast, practically requires people to bring such information along with them wherever they go.

Adopting the State's reasoning would also be tantamount to holding that police officers can search virtually any file on a smartphone. Certainly emails are no more "fundamentally different from" non-digital information than digital photos and videos are. Nor are personal letters or business documents kept on smartphones (or iPads or laptops) fundamentally different from non-digital papers.

---

specify that "the 'place' to be searched is the cell phone." U.S. Br. 24. But there is no reason why the Fourth Amendment's particularity requirement should dissipate in the digital sphere. Nor have magistrates thought so. *See, e.g.*, Search and Seizure Warrant, *In re Search of an Apple I-Phone Model A1332*, No. 1:12-mj-304 (W.D. Mich. Oct. 9, 2012) (identifying specific areas to be searched, including "historical information regarding call activity, 'phone book' directory information, stored voice-mails and text messages").

Even medical and banking records have long existed in tangible form and occasionally been carried by individuals.

To the extent the State's proposed formula has any capacity to limit searches of smartphones, it is anyone's guess how the formula would apply to numerous types of information commonly found on such devices. Does the Facebook app contain fundamentally different information from the non-digital world? How about an online dating app? Or Confession, an app supported by the Vatican that allows Catholics to record sins and examine their conscience?[10] Police officers and others involved in the criminal justice system need these answers now, not years into the future through endless app-by-app litigation.

2. The United States tenders three different limitations of its own, but none works.

a. Contrary to the United States' contentions (Br. 28-30), a rule limiting smartphone searches to situations when "officers reasonably believe that a phone contains evidence of the offense of arrest" would lack any basis in precedent and, at any rate, would not meaningfully curtail searches. As Justice Scalia explained in *Thornton*, the "reasonable belief" exception is "limited, of course, to searches of motor vehicles, a category of 'effects' which give rise to a reduced expectation of privacy." 541 U.S. at 631 (opinion concurring in judgment). Private papers on smartphones, by contrast, are people's "dearest

---

[10] *Catholic Church Gives Blessing to iPhone App*, BBC (Feb. 8, 2011), http://www.bbc.com/news/technology-12391129.

property," *Entick v. Carrington*, (1765) 95 Eng. Rep. 807, 817-18 (K.B.) – information that is subject to *enhanced* expectations of privacy. It is therefore unsurprising that no historical authority allows exploratory searches of such material for mere evidence of crime. *See Thornton*, 541 U.S. at 631 (Scalia, J., concurring in judgment); Petr. Br. 32, 34-36.

Applying a reasonable-belief test to smartphones would also swallow a general rule prohibiting warrantless searches. The United States asserts that "most traffic offenses" and other minor offenses "would not justify a search of an arrestee's cell phone under [the reasonable-belief] standard." Resp. Br. 29. But the Government ignores that smartphones contain information relevant to the most typical of all traffic offenses: speeding. Petr. Br. 41; *see also Jones*, 132 S. Ct. at 963 (Alito, J., concurring in judgment) (phone GPS tracks a user's "speed of movement"); Sahas Katta, *How My Smartphone Got Me Out of a Speeding Ticket in Traffic Court*, Skatter Tech (Feb. 21, 2011) (describing case in which such evidence was used).[11] The United States also contends that a hunch that a person arrested for possessing firearms might have photos relevant to that charge satisfies the reasonable-belief test. U.S. Br. 30-31. If so, then surely a hunch that a person arrested for DUI (the most common misdemeanor for which people are arrested, *see* Petr. Br. 2 n.2) might

---

[11] http://skatter.com/2011/02/how-my-smart-phone-got-me-out-of-a-speeding-ticket-in-traffic-court/.

have relevant photos from earlier that evening would satisfy that test as well. One could go on and on.

The only logical inference, therefore, to be drawn from the United States' comments respecting traffic and other minor offenses is that even the Government senses how outrageous it would be to search people's smartphones incident to arrest for such offenses. But any such carve-out would run headlong into this Court's precedent. As this Court explained in *Robinson*, at the behest of the United States itself, "all custodial arrests" – no matter how petty the offense – must be "treat[ed] . . . alike for purposes of [the search incident to arrest doctrine]." 414 U.S. at 235.

b. Although Arizona and other states urge this Court to eschew any holding that "would require officers to make impromptu decisions regarding the appropriateness of a particular search based upon a myriad of factors associated with each particular arrest," Br. 2-3, the United States next suggests that officers should be permitted to search "the areas of the phone reasonably related to finding evidence relevant to the crime of arrest, identifying the arrestee, and protecting officers." U.S. Br. 30. Such an "area by area" approach would generate an administrative nightmare. Data on smartphones is increasingly interwoven and impossible to separate. A "contacts" file, for example, typically culls and integrates data from the phone's social networking apps; a calendar can sync with GPS-tracking software; and "text" messages now include private photos, videos, business and medical notifications, and more. How would an officer decide which of a phone's various apps with overlapping information

would be appropriate to search? How far back in time within each app can a search go? Can links to external information found during these searches be activated? The United States provides no answers.

c. Lastly, referencing *Chimel*'s "spatial limit" on searches incident to arrest, the United States argues that remotely stored data, as opposed to data saved on a phone, is physically outside the arrestee's "reaching distance" and thus off-limits. U.S. *Wurie* Br. 43-44. But this analogy to an arrestee's physical environment is nonsense. That digital information is stored remotely does not make it any less accessible to the holder of a phone.

In any event, precluding officers from "affirmatively us[ing]," U.S. Br. 34, smartphones to examine digital material stored elsewhere would not meaningfully curtail the scope of smartphone searches. Smartphones continually pull down new data on their own from remote servers. Smartphones also are designed so that "the data that is stored on the phone and the data that is stored in the cloud and available on the phone are often indistinguishable." Br. of EPIC 13; *see also* Apple, iOS Human Interface Guidelines 102 (2014) ("Ideally, users don't need to know where their content is located and they should seldom have to think about which version of the content they're currently viewing."). So unless police officers permanently disconnect the phone from its network before conducting any search, they will have no way of knowing whether data displayed on a phone is stored locally or remotely.

Even after a phone has been disconnected from its network, information on apps that comes from remote sources will still usually be on the phone.

Whenever such an app has been launched, it "store[s] at least temporary copies of the accessed material on the phone itself." Resp. Br. 55. Thus, even under the United States' remote-storage restriction, individuals' business, medical, banking, and other highly sensitive information would still be exposed to warrantless exploratory searches.

II. The Search Of Petitioner's Phone At The Stationhouse Was Too Remote From His Arrest To Qualify As A Search Incident To Arrest.

Neither of the State's arguments in defense of the remoteness of the stationhouse search of petitioner's smartphone withstands scrutiny.

A. At least insofar as the stationhouse search of petitioner's smartphone occurred far away from "the *immediate* vicinity of the arrest," *Shipley v. California*, 395 U.S. 818, 819-20 (1969) (per curiam) (quoting *Stoner v. California*, 376 U.S. 483, 486 (1964)), the State does not dispute that the search contravened the remoteness limitation enunciated in this Court's cases. *See* Petr. Br. 44-47 (discussing these cases). But, relying on *Edwards*, the State argues that this remoteness limitation does not apply to items seized at the scene from arrestees. Resp. Br. 25-28.

As petitioner has explained, the dispositive inquiry under *Edwards* is not whether the item was on the arrestee's person when arrested, but instead whether the item was still in his possession "at the place of detention" – and thus still subject to *Chimel*'s

justifications – when seized and inspected. *Edwards*, 415 U.S. at 807; *see* Petr. Br. 48-51.[12] Any other distinction would be completely arbitrary. Whatever reason may exist, with respect to searches in the field, for distinguishing between items seized from persons and their grab areas, there is no difference, with respect to searches at the stationhouse, between an item that was taken two hours ago from an arrestee's pocket and one that was in a piece of luggage or sitting beside him. Petr. Br. 51.

The State responds that "it is hard to see the benefit . . . of insisting that every aspect of the search take place at once, or at the initial scene." Resp. Br. 26. But just as with the automobile searches at issue in *Thornton* and *Gant*, this argument mistakenly "assumes that, one way or another, the [warrantless] search must take place." *Thornton*, 541 U.S. at 627 (Scalia, J., concurring in judgment). Where "sensible police procedures," *id.*, dictate doing the search later at the police station, there is no reason not to apply the traditional warrant requirement. And in this context, good police work nearly always dictates that searches deep into smartphones take place at the station. *See* Br. of Crim. Law Profs. 10-11; NIST Draft Guidelines 37 (flowchart repeatedly instructing police to wait to search devices).

---

[12] The United States notes that the clothing in *Edwards* was "later subjected to laboratory analysis." U.S. Br. 32. The defendant did not challenge that action, which in any event would not have raised privacy concerns anywhere near the ones at issue here.

B. It makes no difference that petitioner's smartphone was "first examined at the original scene." Resp. Br. 26. This Court has never adopted the "second look" doctrine on which the State relies. Nor should it. That police have grounds at one moment to conduct a warrantless search does not obviate the need for a warrant in perpetuity. A non-digital analogy is instructive: When the police arrest someone in his home, they may search the area within the arrestee's reach and conduct a protective sweep. But they may not return two days later for a second warrantless search. *See Mincey v. Arizona*, 437 U.S. 385 (1978).

At any rate, whatever the law may be when the police reexamine information that was "fully exposed" to them at the original scene, *United States v. Burnette*, 698 F.2d 1038, 1049 (9th Cir. 1983), an initial cursory glance at a few texts on a smartphone cannot possibly justify a later search of other files on the phone. In such an instance, the later search is really the *first* look, not the second.

CONCLUSION

For the foregoing reasons, the judgment of the California Court of Appeal should be reversed.

Respectfully submitted,

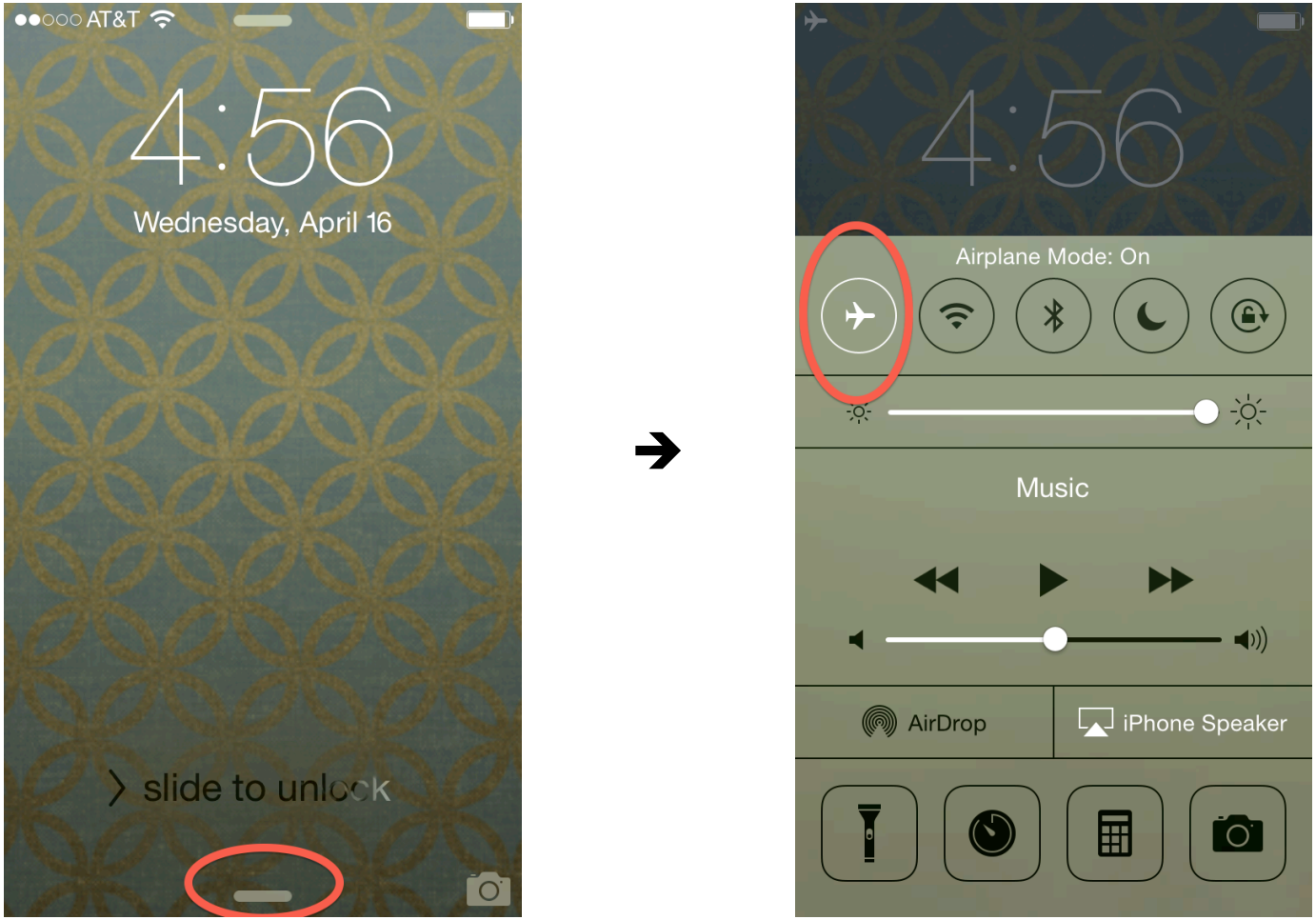
Patrick Morgan Ford
LAW OFFICE OF PATRICK MORGAN FORD
1901 First Avenue
Suite 400
San Diego, CA 92101

Donald B. Ayer
JONES DAY
51 Louisiana Avenue, NW
Washington, DC 20001

Jeffrey L. Fisher
Counsel of Record
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

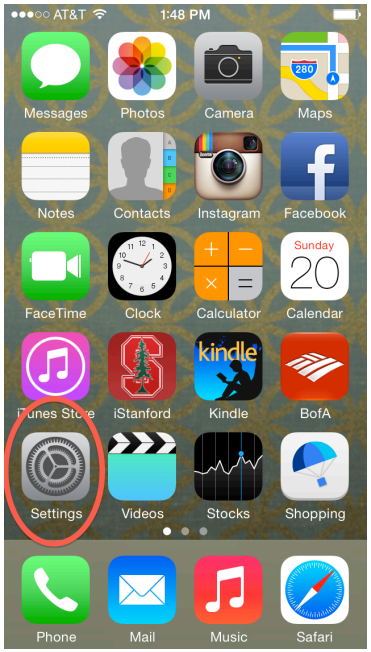
April 22, 2014

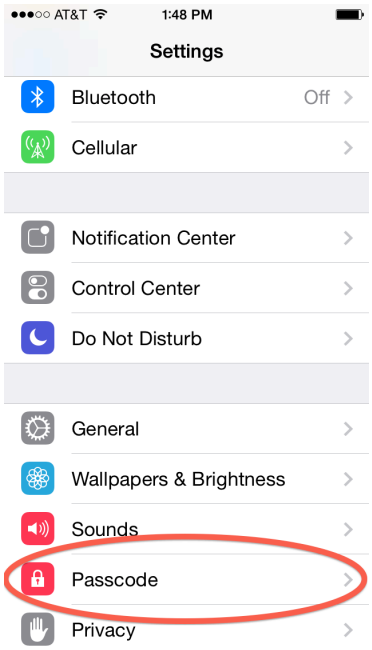
Appendix A



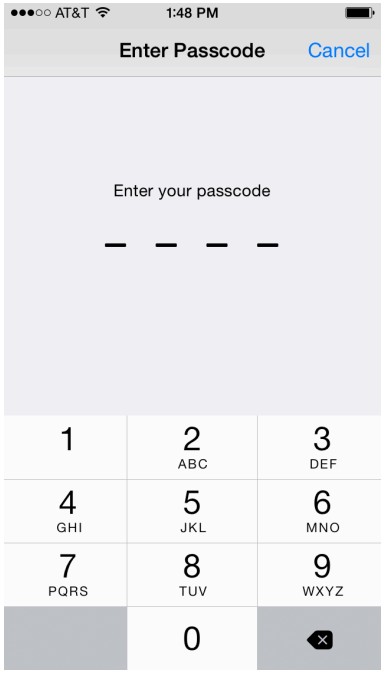
The two steps necessary to put an iPhone in airplane mode, regardless of whether it is locked.

Appendix B

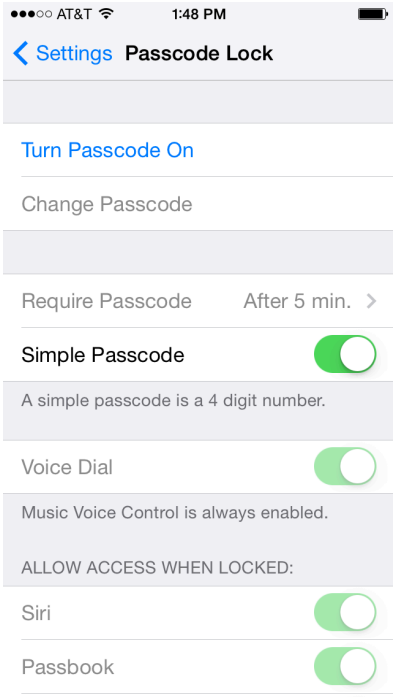




Password enabled

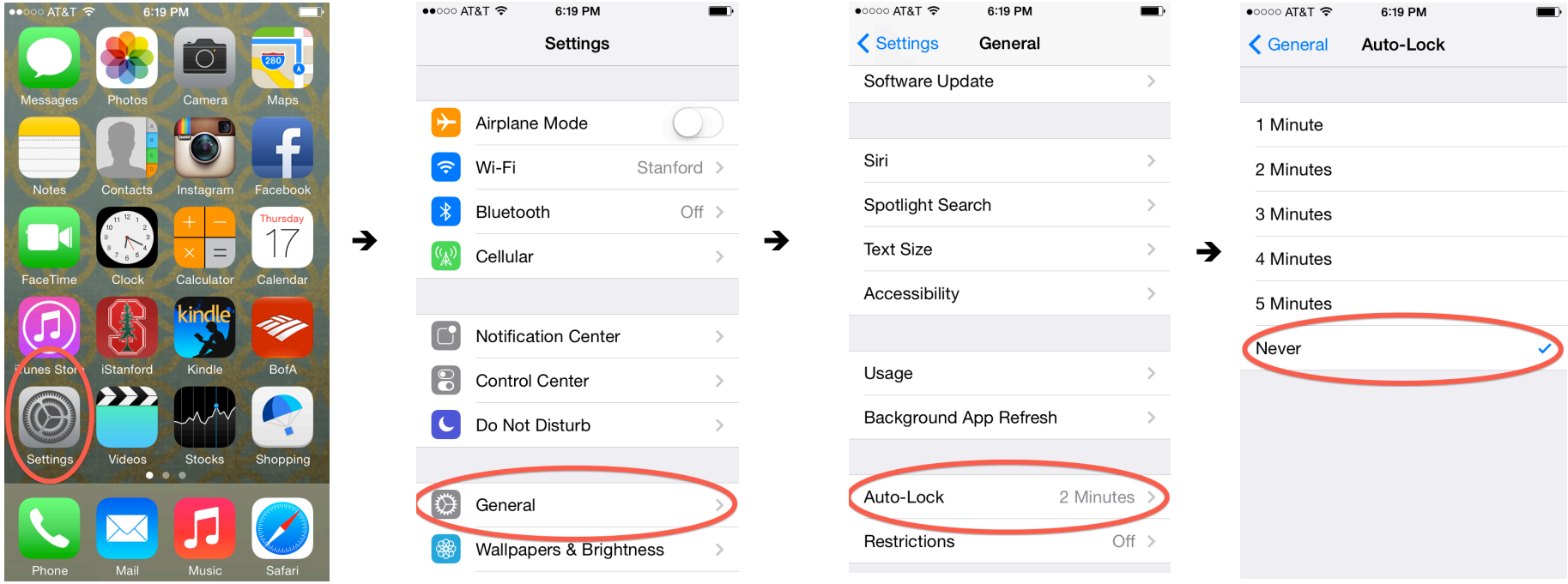


Password disabled



The two steps necessary to determine whether an iPhone has password protection.

Appendix C



The four steps necessary to disable the auto-lock feature through an iPhone's settings.