Arrest, Search and Investigation

Riley v. California, 573 U.S. __ (June 25, 2014). The police may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. This decision involved a pair of cases in which both defendants were arrested and cell phones were seized. In both cases, officers examined electronic data on the phones without a warrant as a search incident to arrest. The Court held that "officers must generally secure a warrant before conducting such a search." The Court noted that "the interest in protecting officer safety does not justify dispensing with the warrant requirement across the board." In this regard it added however that "[t]o the extent dangers to arresting officers may be implicated in a particular way in a particular case, they are better addressed through consideration of case-specific exceptions to the warrant requirement, such as the one for exigent circumstances." Next, the Court rejected the argument that preventing the destruction of evidence justified the search. It was unpersuaded by the prosecution's argument that a different result should obtain because remote wiping and data encryption may be used to destroy digital evidence. The Court noted that "[t]o the extent that law enforcement still has specific concerns about the potential loss of evidence in a particular case, there remain more targeted ways to address those concerns. If the police are truly confronted with a 'now or never' situation—for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt—they may be able to rely on exigent circumstances to search the phone immediately" (quotation omitted). Alternatively, the Court noted, "if officers happen to seize a phone in an unlocked state, they may be able to disable a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data." The Court noted that such a procedure would be assessed under case law allowing reasonable steps to secure a scene to preserve evidence while procuring a warrant. Turning from an examination of the government interests at stake to the privacy issues associated with a warrantless cell phone search, the Court rejected the government's argument that a search of all data stored on a cell phone is materially indistinguishable the other types of personal items, such as wallets and purses. The Court noted 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" and that they "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." It also noted the complicating factor that much of the data viewed on a cell phone is not stored on the device itself, but rather remotely through cloud computing. Concluding, the Court noted:

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.
>
> Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.

(Slip Op at. p. 25). And finally, the Court noted that even though the search incident to arrest does not apply to cell phones, other exceptions may still justify a warrantless search of a particular phone, such as exigent circumstances.