At least five intersections with other Fourth Amendment doctrine will limit these protections. First, observing plaintext in plain view is not a search. Something is in plain view if police view it from a lawful position, its incriminating character is immediately apparent, and police have lawful access to it.[[1]](#footnote-1) Similarly, there is no reasonable expectation of privacy in information in plain view even if it is encrypted at other times or elsewhere.

Second, poorly or improperly encrypted information deserves less protection. There is no reasonable expectation of privacy in an otherwise private yard viewable only by low-altitude aircraft.[[2]](#footnote-2) Similarly, if a suspect uses weak encryption or exhibits security deficiencies that a novice hacker could exploit, protections are weakened. But if law enforcement accesses encrypted data using tools unavailable to the general public, then *Kyllo* is more applicable.

Third, it may matter who does the encrypting. Under third-party doctrine, you have no reasonable expectation of privacy in information shared with others.[[3]](#footnote-3) The Supreme Court limited third-party doctrine in *Carpenter v. United States*, holding that it did not extend to 127 days of location data shared warrantlessly with a wireless carrier.[[4]](#footnote-4) And the Court signaled interest in strengthening Fourth Amendment protections for sensitive data shared with third parties.[[5]](#footnote-5) But under current doctrine, if a third party encrypts your data but can lawfully access the plaintext or key, then they can warrantlessly share either with law enforcement.

Fourth, protections for encrypted information will change at the border. For example, the Ninth Circuit held that forensic examination of physical devices at the border, to include the use of software that accesses encrypted files, requires only reasonable suspicion.[[6]](#footnote-6)

Fifth, abandoned encrypted information may get less protection. In general, abandoned property has no Fourth Amendment protection,[[7]](#footnote-7) including discarded trash.[[8]](#footnote-8) Courts are now wrestling with whether to apply abandonment doctrine to discarded cell phones. One court applied *Riley* protections to an abandoned phone that was secured and password-protected,[[9]](#footnote-9) but several courts did not extend those protections to unsecure, abandoned phones.[[10]](#footnote-10)

1. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993). [↑](#footnote-ref-1)
2. California v. Ciraolo 476 U.S. 207, 214 (1986); Florida v. Riley, 488 U.S. 445, 450 (1989). [↑](#footnote-ref-2)
3. United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Maryland, 442 U.S. 735, 743-44 (1979). [↑](#footnote-ref-3)
4. 138 S. Ct. 2206, 2217 (2018) (reasoning that when *Smith* was decided “few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.”). [↑](#footnote-ref-4)
5. *Id.* (expressing concern with time-stamped location data because it “provides an intimate window into a person's life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” (quoting United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring))). [↑](#footnote-ref-5)
6. United States v. Cotterman, 709 F.3d 952, 962-63, 963 n.9 (9th Cir. 2013). [↑](#footnote-ref-6)
7. Abel v. United States, 362 U.S. 217, 241 (1960). [↑](#footnote-ref-7)
8. California v. Greenwood, 486 U.S. 35, 40 (1988). [↑](#footnote-ref-8)
9. State v. K.C., 207 So. 3d 951, 955 (Fla. Dist. Ct. App. 2016). [↑](#footnote-ref-9)
10. United States v. Small, 944 F.3d 490, 503-04 (4th Cir. 2019) (holding that an unsecure phone discarded by defendant while fleeing a crash was abandoned); United States v. Crumble, 878 F.3d 656, 660 (8th Cir. 2018) (holding that abandonment is a case-specific exception for warrantless search allowed by *Riley*); State v. Samalia, 375 P.3d 1082, 1089 (2016) (holding that an unsecure phone could be warrantlessly searched). [↑](#footnote-ref-10)