# Use Case: Law Firms

Protecting sensitive information in the era of smartphone surveillance

## OVERVIEW

Confidential and sensitive conversations, such as attorney client privileged communications or work product privileged communications, relating either to the firm's day-to-day operations or privileged communications, can be breached at anytime, anywhere or in any unsuspecting circumstance. But ensuring instant access to privileged information is essential and necessary to provide legal advice.

Because each lawyer is responsible for securing his or her communications, whether by email, cell or text, with the client, that means they are also responsible for securing their mobile devices against unwarranted surveillance.

Maintaining secure communications in this ever changing electronic world is an ethical and legal obligation for lawyers and their firms. To meet these evolving threats, Privoro offers security for large, medium and small firms to guard against those who seek to breach the attorney client and work product privileged communication. Compromised smartphones must be protected against all forms of confidential communication breaches that, if not eliminated, can jeopardize the firm's reputation and expose it to legal malpractice.

## CHALLENGE

Smartphone vulnerabilities make them the attack surface of choice for malicious actors of all sorts. This is due, in large part, to the fact that compromised smart-phones can be turned into listening and spying devices – giving unwarranted third parties front-row access to the information shared around them. Known as data in vicinity, assets like sensitive documents, conversations, interviews, testimony and depositions can be recorded or captured via smartphones – stolen without detection. In addition to case-specific audio and visual detail, firms also run the risk of having operating procedures, negotiating tactics, client lists and partner compensation swept up in this type of surveillance.

## SOLUTION

Establishing and enforcing a digital device policy, including where and when smartphones are permitted, is a good first step. But even in the most controlled legal environments, with policies in place, failure to secure the microphones and cameras of mobile devices invites potential risk. With the Privoro SafeCase, firms can take control of device sensors with high-security, intelligent protections that work around the vulnerabilities of smartphones, while still allowing most phone functionality, like email, messaging and cloud storage. SafeCase elevates the security posture of the organization while protecting the privacy of the mobile workforce.

PRIVORO®