

Stanford Technology Law Review
Symposium
Beyond a Physical Conception of the Fourth Amendment:
Search and Seizure in the Digital Age

Richard Salgado
Lecturer at Law Stanford Law School†

Title: Anticipatory Electronic Surveillance in Anglo-American Law

The principles behind the Fourth Amendment's Search and Seizure clause are found throughout Anglo-American jurisprudence. This body of law reflects a history of attempting to harmonize the seemingly conflicting governmental goals of communication privacy on the one hand, and protecting the public safety and national security on the other. Nations adopt surveillance doctrines, driven largely by the realities of the technology. As technologies change, assumptions behind doctrines can become outdated.

Digitalization of voice and data communications is a watershed moment in technological change that requires a refinement and better definition of core concepts behind surveillance law. A doctrine common in the laws of the United States, United Kingdom, Ireland, Australia and New Zealand, for example, is that copying communications stored in a location at a moment in time is generally viewed less intrusive on the privacy of the target than is the ongoing “interception” of communications over time that transit that location. Accordingly, these nations have adopted legal constructs that differentiate based on the means of communications collection. Under these laws, government agencies generally place greater limits on surveillance that constitutes interception of communications than “mere” collection of stored communications.

The digitalization of communications, however, necessarily means that all such communications are in some sense in a “stored” state at various and numerous points along the communications path. Voice and electronic communications alike now travel across digital networks, at times resting, if only for a nanosecond, in static memory. This technological change, often referred to as store-and-forward, has profound implications for search and seizure law. If the degree of legal protection of a communication rests solely on whether it was collected while in a stored state, then the law can be easily (and even inadvertently) gamed simply by choice of surveillance technology. An eavesdropper can avoid the more onerous requirement and limits of intercept law by placing a data-capture device at a point in the transmission path where communications come to rest momentarily before continuing to the destination. The device, laying in wait to grab communications during those fleeting moments of storage, will achieve the same end as would a similar device that captures data in motion, but without the need to honor the legal protections regulating an interception.

Behind the stored-versus-intercept doctrine is the recognition that constant, ongoing and inevitable surveillance of a space more profoundly intrudes upon privacy than searching

that same space at a discrete moment in time for evidence that happens to be there at the moment of the search. Defining the precise contours of when the acquisition of a communication is deemed an intercept and when it is not should not turn on its storage state or its location. Rather, the focus should more closely reflect the rationale that there is a greater privacy invasion when one sits in the transmission path, monitoring all that passes in an ongoing surveillance effort. In this model, there is an intercept when communications are collected by a device monitoring, in an ongoing, prospective manner, communications that flow into the space. On the other hand, historical collection, collecting only the data that reside in the space at the precise moment of the search does not constitute an interception.

As the courts and legislatures in the Anglo-American countries adjust to this profound technological change, there may be a temptation to move to another rule. For example, one could define an intercept to mean the acquisition of a communication anytime before it reaches the location from which it can be collected by the intended recipient, regardless of the means by which the communication is collected. The rule could be that there is an interception of email, for instance, if the email is copied anytime before it reaches the inbox. This, however, misdirects attention to the space from which the data were acquired and diverts the focus from whether intrusive means were used to collect the data. Under that rule, if one deployed a device that constantly monitored an inbox and copied any new incoming messages, there would be no intercept merely because the data were in a particular space. Looking to the ongoing, forward-looking nature of the acquisition provides a more rational and crafted test suited to better protect the underlying privacy interest.

† The statements expressed herein should not be taken as a position or endorsement of Yahoo! Inc. or its subsidiaries and may not reflect the opinion of their affiliates, joint ventures or partners.