

THURSDAY, MARCH 17, 2022

GUEST COLUMN

California's feeble privacy right is cold comfort

By Brandon V. Stracener
and David A. Carrillo

San Francisco's District Attorney Chesa Boudin recently revealed that the city's police department has a practice of saving DNA from crime victims in a database, which can be used to identify them as suspects in unrelated crimes. Boudin charged that this practice violates California's constitutional privacy guarantee. Morally wrong as it may be, courts are unlikely to find that this practice violates our anemic state constitutional privacy right.

That's because California's constitutional privacy right is a failed promise. In 1972 California voters passed Proposition 11 and amended article I, section 1 of California's constitution to include a right to privacy. This Privacy Initiative was intended to combat government efforts to collect information about us: proponents were concerned that Californians lacked any defense against the government's ability to employ technology to build "cradle-to-grave" dataprofiles of citizens. The ballot arguments warned that modern technology "is capable of monitoring, centralizing and computerizing this information which eliminates any possibility of individual privacy." The voters in 1972 intended the new right to be a shield against state surveillance, corporate record collection, and government snooping.

That sounds like just the reme-

dy for a government practice that takes vital personal identifying information given for a limited purpose and instead uses it for the comprehensive data profiling that Proposition 11 was concerned about. And there might be a viable California constitutional privacy claim here if courts interpreted the law as the 1972 voters intended.

Yet as explained in "California Constitutional Law: Privacy" (in San Diego Law Review Volume 59 in April), after a brief heyday courts weakened California's constitutional privacy right to its present sickly state. The voters who enacted the Privacy Initiative intended to value privacy at a high level and require invaders to justify intrusions by showing a compelling public need. But courts were concerned about how businesses might struggle if they needed to ask customers for consent for their data, and how burdensome it would be for the government to justify its data collection. To make life easier for commerce and governance, courts gutted Proposition 11 by setting a high bar for plaintiffs to state a claim, giving defendants multiple opportunities to prevail on summary judgment, and rebalancing the interests so that privacy fell from a fundamental constitutional liberty to being on par with a store's interest in collecting shopping data.

Along the way, courts divided privacy into two categories: informational and autonomy. Informational privacy includes things

like Social Security numbers, cellular call data, and geolocation tracking. Autonomy privacy covers physical invasions, such as pat-down searches and obtaining bodily samples. Collecting DNA from crime victims and using it for unrelated purposes has elements of both categories, but California's constitutional privacy right probably protects neither.

An article I, section 1 privacy claim likely fails here because a consensual cheek swab will not establish the threshold element of a reasonable expectation of privacy. Compulsory physical samples were upheld in *Hill v. NCAA* (1994) 7 Cal. 4th 1, so a court is unlikely to view a voluntary sample as problematic. And even serious informational or autonomy privacy invasions can be justified by a

mere legitimate interest. *See, e.g., Loder v. City of Glendale* (1997) 14 Cal.4th 846 (autonomy); *Lewis v. Superior Court* (2017) 3 Cal.5th 561 (informational). Courts have already recognized that collecting DNA serves compelling state interests in prosecuting crimes accurately and rectifying erroneous convictions. *Alfarov. Terhune* (2002) 98 Cal.App.4th 492. Although article I, section 28 gives crime victims the right to be treated with respect for their "privacy and dignity," one lacks an expectation of privacy in something freely given. And California's Truth in Evidence provision would probably protect a DNA match from suppression. *See People v. Robinson* (2010) 47 Cal.4th 1104.

Thus, there are two banes in today's constitutional privacy stan-

Brandon V. Stracener is a senior research fellow at and **David A. Carrillo** is the executive director of the California Constitution Center at Berkeley Law. The views expressed here are solely their own and not those of their respective employers.



standard: the difficulty of showing a protected interest, and the ease of establishing a countering interest. The court-created threshold elements bar most constitutional privacy claims by forcing plaintiffs to prove a serious invasion of a protected privacy interest. But because courts reject around 80% of constitutional privacy claims there's scant caselaw defining such interests. And even if a plaintiff shows a significant interest, there's almost always an equivalent countervailing interest. The upshot is that neither an autonomy nor an informational privacy claim is likely to succeed here.

Nor can a statutory remedy fill the gap left by this judicial dilution of California's constitutional privacy right. For example, Penal Code section 680 purports to protect sexual assault victim DNA, but its sole remedy is writ relief to inform the victim of the sample's status. That's a poor alternative to a constitutional remedy.

Making crime victim DNA available for general purposes in government databases has many negative implications. It runs contrary to common sense and a person's reasonable subjective expectation that something given for a specific and beneficial

purpose will not boomerang back on the giver — if I let you borrow my car, I don't expect you to run me over with it. The practice raises serious policy concerns about whether citizens can ever interact with the government without waiving all privacy rights. And deep moral consequences flow from discouraging crime victims from coming forward. Those concerns are particularly acute in the sexual assault context, which already features under-reporting partly because the legal process is so prone to re-traumatizing victims.

The takeaway here is "anything you tell us can and will be used

against you." This episode should remind us that Californians have less privacy than they assume — far less than one expects from a state constitution that guarantees privacy. That's largely due to hostile judicial interpretation. To their credit, California's legislature and citizen lawmaker Alastair Mactaggart have filled some resulting gaps, but a statutory remedy is never a substitute for a constitutional right. Just remember that if you tell the government something, California's constitutional privacy right probably will not prevent the government from using that information against you.