IN PRACTICE

Disruptive innovation, meet the common law

As technology races ahead, it sometimes crashes into longstanding constitutional law doctrines

Ben Feuer

Ben Feuer is an appellate attorney with the California Appellate Law Group (www.calapplaw.com) in San Francisco, where he represents businesses and individuals in civil appeals. He is the chair of the appellate section of the Bar Association of San Francisco's Barristers Club, and formerly served as a law clerk at the Ninth Circuit. He can be reached at ben@calapplaw.com.

Constitutional Law

First of two parts

Silicon Valley loves the concept of "disruptive innovation." The term applies when a new product or service enters a market and innovates in ways that render the normal behavior of existing participants obsolete. A great example is Netflix, which innovated a new concept of video delivery and pricing that, through technology, fatally undermined the "be kind, rewind" model of Blockbuster and Hollywood Video. Likewise, car sharing services like Uber, Lyft and Zipcar are disrupting the well-entrenched radio-dispatched taxi market by employing new technologies to allow for more efficient methods of dispatching vehicles.

The law does not like disruptive innovation. To the contrary, the common law system of legal authority operates on a principle of gradual innovation, changing slowly over time, always by drawing on analogies to similar cases from the past. In many ways, that analogizing is the defining component of common law, creating the law's balance between stability (from continuity to the past) and flexibility (from applying past lessons to modern factual situations).

The downside to the common law is that its analogical nature makes it fundamentally retrospective. Accordingly, the common law can't always keep up with disruptive changes brought by technology, sometimes leading courts that don't fully understand the nuances of an innovation to a wrong result.

WHAT'S IN "PLAIN VIEW" ON A COMPUTER SCREEN?

First, the Ninth Circuit took on the meaning of the "plain view" exception in the information age in its en banc decision in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010). That appeal arose out of the Major League Baseball doping scandal, when federal investigators discovered evidence that 10 baseball players tested positive for illegal steroids. Based on that evidence, the government obtained several warrants for drug-testing records related to those 10 players. It executed the warrants on the laboratory that drug-tested baseball players, demanding all records for the players subject to the warrant.

Had the laboratory kept a filing cabinet that allowed government agents to simply pull out the files for the 10 players, the appeal might never have arisen. But when investigators arrived at the lab, they discovered the records were stored not in carefully labeled filing cabinets, but instead on computer hard drives along with thousands of other records. Lacking the time and capacity to sort through all the hard drives on the scene for information responsive to the warrant, the government seized everything. The FBI then examined every single file on the hard drives, because, it later explained, information responsive to the warrant could be given any file name and contained in any file type.

In the course of that search, the FBI discovered a Microsoft Excel file that contained a worksheet listing the names of all the baseball players that laboratory had identified as testing positive for steroids—the 10 subject to the warrant, plus many more. After reviewing the entire list, the FBI obtained a warrant authorizing the seizure of further files related to the other names on that list. The gesture was something of a formality, however, because the FBI already had those files in its possession anyway, and had already reviewed them in searching for records of the 10 players previously identified.

The Major League Baseball Players Association and drug-testing laboratory filed motions seeking the return of the files, to mixed results. On appeal, the Ninth Circuit court ordered the files returned because the government did not disclose all relevant information when obtaining its warrants. But the court's per curiam, unsigned majority opinion ended with the recognition of a novel problem: "Once a file is examined, the

wrong result.

In 1981, for example, the U.S. Court of Appeals for the Ninth Circuit ruled that Sony could be held liable by television broadcasters for copyright infringement resulting from home use of its Betamax VCR. The Ninth Circuit based its ruling on statutes permitting audiocassette recording, which it determined was a right unique to audiocassettes. If not later reversed by a closely divided U.S. Supreme Court, the Betamax ruling might have ended the nascent videocassette recording industry then and there.

The Internet age has rapidly accelerated technological development and its intrusion into everyday life. In some instances, it has redefined whole industries and basic paradigms. (When was the last time you stopped to ask for directions?) And the speed of change continues to creep up. As it has, a few judges have begun to recognize that certain technological advances are so disruptive to existing norms that analogies with the past don't necessarily hold up under close scrutiny. **In other words, these judges concluded that applying the most analogous precedent, as the common law usually expects, results in an outcome that while correct on paper, is doubtlessly wrong given the purpose of the underlying law and the nuances of the technology at issue.**

Practice Pointer

HOW DO YOU WRITE "FOURTH AMENDMENT" IN BINARY?

One of the most visible areas in which technology has challenged the common law's ability to keep up is Fourth Amendment search and seizure jurisprudence.

The Fourth Amendment to the U.S. Constitution prohibits "unreasonable search and seizure," which courts have interpreted to prohibit search and arrest absent a warrant or the presence of an exception to the warrant requirement. Any warrant, moreover, must be based "upon probable cause" and "particularly describ[e] the place to be searched, and the persons or things to be seized."

In recent years, technological advances have raised questions about when, precisely, the government needs a warrant to conduct a search, or when an exception to the warrant requirement applies. In particular, courts have struggled with the "plain view" exception (permitting warrantless seizure where contraband lies in the plain view of a police officer conducting an otherwise lawful search), the "non-private information" exception (permitting seizure of information about which the owner lacks a reasonable expectation of privacy), and the "search incident to arrest" exception (permitting seizure of objects on the body of an arrested individual).

As the fractured opinions of appellate courts dealing with these difficult situations make clear, when it comes to technology, the simple application of a common law analogy can lead to unsatisfactory results.

government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization to search some computer files therefore automatically becomes authorization to search all files in the same subdirectory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media. Where computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there." Ultimately, "seizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions."

As a solution, the court applied circuit precedent from the pre-networked 1980s, in the common law way, to hold that where the government seizes large quantities of intermingled files, it should have a magistrate or other third party sort through the data to ensure the government receives only data responsive to the warrant.

But the court did not explain why a magistrate reviewing swept data could not or would not immediately reveal apparent evidence of illegality to the police. **Nothing in the Fourth Amendment requires a reviewing magistrate to ignore an email regarding a human trafficking shipment or ongoing child abuse that she finds during her search, even if unrelated to the unlawful doping at issue in the warrant.** Indeed, how could a magistrate of conscience searching for evidence of illegal steroid use ignore evidence she comes across of child pornography or stolen state secrets?

Practice Pointer

A concurrence authored by Chief Judge Alex Kozinski attempted to resolve some of these tensions with a set of strict protocols—limiting the use of government technology to discover certain types of files without probable cause, for example, and requiring a carefully delineated search protocol outlined in the warrant application. However, his concurrence found support from only four of 11 en banc judges, and would not have eliminated these issues entirely. (Indeed, another judge refused to join these protocols precisely because they circumvented the usual common law process of gradual innovation.) But in the end, because the *Comprehensive Drug Testing* en banc majority adhered to precedent and common law tradition, it left some substantial tensions in place that adopting the more aggressive Kozinski concurrence might have solved.

The second part of this column will consider two other examples in which jurists have, like Judge Kozinski, rejected the easy application of inadequate precedent when confronted with disruptive technology. It will also point out the very real dangers that can arise when courts aren't open to the truly paradigm-bending effects some technologies can have.

In Practice articles inform readers on developments in substantive law, practice issues or law firm management. Contact Greg Mitchell with submissions or questions at gmitchell@alm.com.

IN PRACTICE

Disruptive innovation puts common law courts in bind

Precedent doesn't always seem to hold up in the face of quickly evolving technologies

Ben Feuer

Ben Feuer is an appellate attorney with the California Appellate Law Group (www.calapplaw.com) in San Francisco, where he represents businesses and individuals in civil appeals, including those involving complex or novel technologies. He is the chair of the appellate section of the Bar Association of San Francisco's Barristers Club, and formerly served as a law clerk at the Ninth Circuit. He can be reached at ben@calapplaw.com.

Constitutional Law

Second of two parts examining the difficulties common law courts face when rapidly advancing technologies differ so greatly from those at issue in case law that the most seemingly on-point precedent doesn't hold up.

Last week, the first part of this column explained that certain technologies have advanced so rapidly that sometimes the process common law courts usually undertake, of analogizing to the closest precedent, does not necessarily work. That is because certain innovations are so disruptive that the closest precedent is only deceptively analogous—a full understanding of the technology's nuances would reveal that it is more fundamentally unlike that which came before it than the simple analogy accounts for. Some judges have addressed that tension head on, like the U.S. Court of Appeals for the Ninth Circuit's Chief Judge Alex Kozinski, who unsuccessfully urged adoption of a detailed set of protocols to guide government searches of voluminous electronic data in 2010's *United States v. Comprehensive Drug Testing*.

Two other recent cases also come to mind in which courts faced technological innovations so disruptive that simple application of precedent created new tensions and deep difficulties, forcing individual judges to step forward to ask whether the technology had advanced far enough that it required a different response altogether.

WHAT HAPPENS WHEN YOUR SECRETS FIT IN YOUR POCKET?

If Judge Leon took a critical eye to strict application of precedent in the face of changing technology, the California Supreme Court wore blinders in 2011, when it considered the effect of changing technology on cellphone searches conducted by police immediately after arrest.

In *People v. Diaz*, 51 Cal.4th 84, the state Supreme Court held that, as part of a "search incident to arrest," the police may seize and later peruse an arrestee's cellphone to find evidence of any kind of wrongdoing, without first obtaining a warrant based on probable cause. In *Diaz*, the police found text messages regarding drug sales, which they later used to prosecute Diaz for narcotics offenses.

In affirming Diaz's conviction, the court applied U.S. Supreme Court precedent from the early 1970s, which permitted the police to search the immediate person of anyone arrested and seize weapons or evidence without a separate warrant. That case, *United States v. Robinson*, 414 U.S. 218 (1973), considered the admissibility of a cigarette packet containing drugs that the police found in an arrestee's pocket, which the arresting officer searched after the arrest without obtaining a search warrant based on probable cause. The court held the search of the pocket and seizure of the cigarette packet passed Fourth Amendment scrutiny, reasoning that the police should be able to ensure their own safety and collect relevant evidence before it can be destroyed and without a court later second-guessing that often split-second decision. **So in *Diaz*, the California Supreme Court began and ended its analysis with the observation that, like Robinson's cigarette packet, the cellphone was Diaz's personal property that the police officers obtained after conducting a *Robinson*-approved search of his pockets after his arrest. The court refused to distinguish between the phone itself and its electronic contents.**

A lone voice, Justice Kathryn Werdegar, dissented on the ground that, given modern technology, a cellphone is much more than a mere object of personal property. Rather, "[t]he potential intrusion on informational privacy involved in a police search of a person's mobile phone, smartphone or handheld computer is unique among searches of an arrestee's person

Practice Pointer

WHICH DIGITAL INFORMATION IS 'PRIVATE'?

Like the *Comprehensive Drug Testing* case, another example of tension created by the difference between the speed of technological innovation and the common law's deliberative rate of change appears in twin 2013 U.S. District Court decisions that concern the National Security Agency's bulk collection of telephone "metadata." Metadata records the time, place, and to/from information for phone calls. The two opinions, by Judge William Pauley in the Southern District of New York, and Judge Richard Leon in the District of Columbia, reached opposite conclusions about the constitutionality of bulk metadata collection.

In 1979, the U.S. Supreme Court held in *Smith v. Maryland*, 442 U.S. 735, that police officers do not need a warrant to install a device at a telephone company's switchboard that records the numbers dialed by a suspect's home telephone, because telephone users do not have an expectation of privacy in the numbers they dial since they necessarily share that information with the phone company when they place a call.

Practice Pointer

Judge Pauley, a Clinton appointee, applied *Smith* in typical common law fashion to hold that the NSA's metadata collection program fell squarely within precedent. **Thus, he ruled that the government did not violate the Fourth Amendment by sweeping up all telephone metadata without a warrant tied to a specific individual and based on probable cause.** Directly invoking *Smith*, Pauley wrote that when a person uses technology that necessarily gives information to a third party, such as a telephone company or Internet email provider, "he forfeits his right to privacy in the information."

Practice Pointer

Around the same time that Judge Pauley issued his opinion, Judge Leon, a George W. Bush appointee, looked closely at the nature of bulk metadata collection and reached the opposite conclusion. **Judge Leon determined that the technology the government employed had advanced so far from where it stood in 1979 that the Supreme Court's opinion in *Smith* had become unmoored from modern practices, in light of the original meaning of the Fourth Amendment.** Unlike the "highly-limited data collection" in *Smith*, Leon explained, the NSA's program involves "almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States" and it "is unlike anything that could have been conceived in 1979." When taken in bulk and pieced together with computers, Judge Leon explained that the data reveals a wealth of personal information, including "familial, political, professional, religious, and sexual associations." In the 1970s, Leon wrote, today's metadata collection technology would have been "the stuff of science fiction."

Leon then asked the critical question, one that applies not just to metadata collection but to an array of common law constitutional doctrines in light of rapidly advancing technologies: "When do present-day circumstances—the evolution of the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply?" In terms of metadata, Judge Leon concluded technology has now reached that point.

Both Judge Leon's and Judge Pauley's decisions, and the tensions they embody, will certainly see further review on appeal.

and effects." That is because today's cellphones, unlike cigarette packets, might contain a person's entire history of electronic correspondence, his or her text messages, contacts, photographs, video: video recordings, bank account data, business documents, diary entries, even the history of where the phone has traveled via GPS. They have become miniaturized filing cabinets for our entire lives, slipped into a pocket. Since *Diaz*, they have become constantly synced to the Internet and cloud-based storage, and offer one-touch access to a person's entire library of private information. Within a decade, Google Glass and similar technologies may record and store video of every minute of life, accessible at all times. Relying on the purpose and text of the Fourth Amendment, rather than shoehorned precedent, Werdegar explained that a "context-dependent balancing of constitutionally protected privacy interests against the police interests in safety and preservation of evidence led the United States Supreme Court, over 30 years ago, to hold searches of the arrestee's person reasonable despite the lack of probable cause or a warrant and despite substantial delay between the arrest and the search." However, "in the very different context of mobile phones and related devices, that balance must be newly evaluated" in a way the majority failed to do. The result of the majority opinion, Werdegar pointed out, is that "it would subject anyone who is the subject of a custodial arrest, even for a traffic violation, to a preapproved foray into a virtual warehouse of their most intimate communications and photographs without probable cause."

Fortunately, the *Diaz* majority will not have the last word on the scope of cellphone searches incident to arrest. In January 2014, the U.S. Supreme Court granted *certiorari* in *Diaz*, and will review the case anew. **It remains to be seen whether the justices at 1 First Street will recognize the difference between a packet of cigarettes and a pocket-sized computer that contains many individuals' brightest hopes, darkest secrets, and most embarrassing selfies.** The justices famously still send printed memos to one another rather than emails. And while age is far from a certain indicator of comfort with technological innovation, the average age of a U.S. Supreme Court justice is nearly 70. Indeed, shortly after the *Diaz* decision, the California Legislature passed a bipartisan bill to require the police to obtain warrants based on probable cause to search a cellphone where not vital to do so immediately—but the state's septuagenarian governor, Jerry Brown, vetoed the measure.

Practice Pointer

However the U.S. Supreme Court rules in *Diaz*, or the appellate courts resolve questions about NSA metadata collection, or magistrates deal with illegalities discovered while segregating files, the tensions created between old precedents and new technologies are only going to accelerate.

The best solutions may not always be easy or obvious, and may not resolve all difficulties at once. But Judges Kozinski and Leon, and Justice Werdegar, have led the charge in recognizing that when technological progress leaps exponentially forward, the common law must sometimes welcome disruptive innovation of its own to keep up.

In Practice articles inform readers on developments in substantive law, practice issues or law firm management. Contact Greg Mitchell with submissions or questions at gmitchell@alm.com.