

THE WALL STREET JOURNAL.

SATURDAY, FEBRUARY 23, 2013

© 2013 Dow Jones & Company, Inc. All Rights Reserved.

MARVELS: HOLLY FINN



The Humane Way to Crack Terrorists

Big data may make 'enhanced interrogation' obsolete

Spooks are sexier than computer programmers. That's one reason we've been paying more attention to "Zero Dark Thirty," the controversial nominee for the Academy Award for best picture, than to the engineers who contribute as much, or more, to our counterterrorism effort.

Let's stop fretting about whether the film endorses torture. (Did "Terms of Endearment"—best picture, 1983—endorse cancer?) What's covert is, by definition, what we're not talking about. That's the bigger story here: the new intelligence methods that are being used, *sub rosa*, right now—and will be used in the future. They may make torture obsolete.

In December, acting CIA Director Michael Morell wrote, "the truth is that multiple streams of intelligence led CIA analysts to conclude that bin Laden was hiding in Abbottabad." Three weeks ago, CIA Director Leon Panetta said: "We put together most of that intelligence without having to resort to [enhanced interrogation]. I think we could have gotten bin Laden without that."

Today, the real action is not at black sites but at well-lit screens. To accomplish missions, the Pentagon contracts with nimble young technology companies: a kind of virtual, creative, bureaucracy-busting CIA West.

There's a tellingly brief passage in "The Finish: The Killing of Osama bin Laden" by Mark Bowden. "The hunt for bin Laden and others eventually drew on an unfathomably rich database," he

writes. "Sifting through it required software capable of ranging deep and fast and with keen discernment—a problem the government itself proved less effective at solving than were teams of young software engineers in Silicon Valley. A startup called Palantir, for instance, came up with a program that elegantly accomplished what TIA [Terrorism Information Awareness program, set up in 2002] had set out to do."

When I met the chief executive and co-founder of Palantir, Alex Karp, recently, he was straightforward: "It is my personal belief that flawless data integration at any kind of scale, with a rigorous access control model, allows analysts to perform operations that are only intrusive on the data. They are not intrusive on human beings." Obviously, Palantir doesn't comment on classified work. But its technological phalanx—processing countless leads, from flight manifests to tapped phone calls, into one resource for people to interpret—is known to have been key in locating bin Laden. The company, founded in 2004, has large contracts across the intelligence community and is enterprise-wide at the FBI. Its first client was the CIA.

The old saying went: If you torture the data long enough, they will confess. Maybe now it should go: If you torture the data well enough, there's no reason to torture people. Against modern, entrepreneurial adversaries, the ability to quickly navigate huge data sets is a real advantage. Fresh anomalies are flagged, connections made, patterns found. The

meaning of any one piece of information changes in a new context. A lobster looks different in the desert.

Does this mean that our government is suddenly outsourcing its spywork to secretive private companies? Not quite. Palantir sells software; government employees use it to untangle information they already collect. The techies don't see those data. Their software can be used to track individuals, but it's the government that decides if it will be.

Technology is no panacea (hacking is a threat). Nor is it infallible. And it can't explain intentions. But systems like Palantir's seem both thorough and durably accountable—with data retention, effective protocols for anonymity and robust privacy protections.

Well used, data eliminate "the need to go beyond the bounds of what should be legitimate actions," says Mr. Karp, who holds a law degree from Stanford and a Ph.D. in social theory from the University of Frankfurt. As he sees it, computer code can help us to uphold our moral code.

By contrast, in "Zero Dark Thirty" and other depictions of "enhanced interrogation," the interrogator, breaking his prisoner, is broken himself: cold, emotionless, machinelike. Today's data-driven covert operations may just let us conclude that torture is not only archaically inhumane—for all involved—but actually obsolete. "In my view," says Mr. Karp, "it's been proven."