Editors: Alessandro Acquisti, acquisti@andrew.cmu.edu | Hugh Thompson, hthompson@peoplesecurity.com

What Happened to the Crypto Dream?, Part 1

Arvind Narayanan | Princeton University

Steven Levy's fascinating 2001 book *Crypto* has the subtitle *How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*.[1] The "code rebels"—a loose coalition of academics, hobbyists, and civil-liberties organizations—did indeed beat the government, causing the earlier restrictions on distribution of cryptographic tools to be largely abandoned. However, this victory seems to have done miserably little to save privacy. In fact, you might look at the early 2000s as the years when digital privacy took a nosedive. Why did Levy and many other observers get it so wrong back then?

For over 2,000 years, evidence seemed to support Edgar Allan Poe's assertion, "human ingenuity cannot concoct a cypher which human ingenuity cannot resolve," implying a cat-and-mouse game with an advantage to the party with more skills and resources. This changed abruptly in the 1970s owing to three separate developments: the symmetric cipher DES (Data Encryption Standard), the asymmetric cipher RSA, and Diffie-Hellman key exchange. For the first time, it was conceivable that someone with modest computing resources could encrypt a message in a way that would resist attack by governments, as long as the key was secret. For the first time, some encryption algorithms came with clear mathematical evidence (albeit not proofs) of their strength. These developments came on the eve of the microcomputing revolution, and computers were gradually coming to be seen as tools of empowerment and autonomy rather than instruments of the state. These were the seeds of the "crypto dream."

Flavors of Crypto

To delve further, we must distinguish different uses of cryptography. The first distinction is between crypto-for-security and crypto-for-privacy. Even though they're similar at the technical level, they're quite different at the social level. The former is used in contexts such as protecting financial transactions (for example, encrypting your credit card number when you buy stuff online). This means that, crucially, the incentives of all parties are aligned toward using crypto to maintain security. And indeed, crypto-for-security has been extremely successful, at least by the criterion that it has been a key to enabling e-commerce. On the other hand, crypto-for-privacy often has social and political goals, and a misalignment of incentives frequently occurs. It's crypto-for-privacy's track record that's of interest to us.

The pioneers of modern crypto clearly recognized both types of goals. In particular, they foresaw that as analog activities moved online, the ease of monitoring, logging, and searching everything meant that we could easily slip into a surveillance society. They saw crypto as a way to thwart this danger and keep the same level of privacy we had in the analog world. I call this, for lack of a better term, "Pragmatic Crypto"—cryptographic enhancements to various digital systems that roughly maintain predigital privacy levels. I'll return to this in part 2 of this article.

In addition, there was a grander crypto dream. Its technical roots are in the work of David Chaum in the early '80s, culminating in his 1985 paper "Security without Identification: Transaction Systems to Make Big Brother Obsolete."[2] Anonymous digital cash, one of the key parts of Chaum's proposal, by itself has political significance in that it offers an alternative to government-backed currencies. But Chaum went further. In his ideas of credentials and "blacklisting without lists," we can see hints of pseudonymous reputation systems. Also, his technique for anonymity revocation contingent on double-spending of a coin can be seen as an example of encoding a social norm or rule (public exposure of thieves) into crypto.

Cypherpunk

The cypherpunk activist movement, which originated in the late

Copublished by the IEEE Computer and Reliability Societies

'80s, took Chaum's ideas and ran quite far with them in terms of rhetoric—in an explicitly subversive direction. For cypherpunks, crypto was at the core of a vision of how technology would cause sweeping social and political change, weakening the power of governments and established institutions. A closely related term is crypto-anarchism, a political philosophy that, in its idealized form, recognizes no laws except those that can be described by math and enforced by code.

Combined with ideas such as information markets and prediction markets, even relatively simple crypto can be quite powerful. One proposal was for markets that would render legal intellectual-property restrictions meaningless. Another was for pervasive untraceable (and hence unregulable) transactions. The vision of crypto fundamentally and inexorably reshaping social, economic, and political power structures is what I call "Cypherpunk Crypto." (Although I've described two extremes, a spectrum exists between Cypherpunk Crypto and Pragmatic Crypto.)

I don't mean to suggest that this belief was mainstream in the crypto or tech communities—when cypherpunk cofounder Tim May handed out copies of his Crypto-Anarchist Manifesto at the 1988 Crypto conference in Santa Barbara, the academics "pretty much ignored him."[3] But the cypherpunks were vocal enough and persuasive enough that *Wired*, for example, was a prominent early champion of the movement.

At least in retrospect, explaining why the cypherpunk dream remains unrealized is like shooting fish in a barrel. To put it simply, democratic governments exist, to a first approximation, with the consent of the governed. So, the demand for technologies that will upset that power balance is quite low. By the same token, however, crypto and anonymity technologies have an important role to play in oppressive regimes. In particular, Tor (www.torproject.org) has found considerable success as a censorship-circumvention tool.

Two more problems with Cypherpunk Crypto seem worth pointing out. First, the more ambitious ideas such as Chaum's proposal of commerce using "card computers" seem to require societal buy-in. This requirement for a critical mass of potential users unhappy with the status quo makes the ideology even more infeasible. In contrast, more modest tools such as email encryption are more incrementally deployable.

Second, to impact the real world, cryptosystems must come into contact with the real world; many convenient abstractions and mathematical assumptions break down at this boundary. For example, software security remains an unsolved problem, which means digital credentials and cash can be stolen with little recourse available to the victim. Also, anonymous digital markets for physical goods are useless if the goods aren't actually shipped, so such systems still must contend with law enforcement.

Rebirth?

Some have claimed that Bitcoin (http://bitcoin.org) and WikiLeaks represent a rebirth of the cypherpunk dream. I find this questionable. Although Bitcoin is a fine technology with interesting niche uses, it so far has had essentially no societal impact. The fact that its more prominent uses such as Silk Road (an online black market) target fringe elements reinforces my point in the previous section.

WikiLeaks is more complicated. Like Cryptome (www.cryptome.org), it has played a valuable role in shining the light on abuses of power, albeit a far cry from cypherpunk rhetoric. And crypto has indeed contributed to its success, although this impact shouldn't be overstated. The organization itself derives its protection primarily from Sweden's laws rather than anonymity technologies. On the other hand, cryptographic anonymity does seem to be a factor in some whistleblowers' decisions to take that step.

The lesson, I think, is reassuring. Crypto and other technological tools have a role to play in keeping power in check, whether in protecting those resisting authoritarian regimes or in bringing more transparency to democratic ones. On the other hand, the evidence doesn't support an overly technologically determinist view in which crypto has its own logic that's powerful enough to reshape society against the collective will. ■

Acknowledgments

I'm extremely grateful to Joseph Bonneau, Ed Felten, and Vitaly Shmatikov (in no particular order) for comments on a draft, and to the audience at my talks at the Electronic Frontier Foundation and Princeton for useful feedback. Any errors, opinions, and omissions are my own.

References

1. S. Levy, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*, Penguin Putnam, 2002.
2. D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Comm. ACM*, vol. 28, no. 10, 1985, pp. 1030–1044.
3. A. Greenberg, *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information*, Dutton Adult, 2012.

Arvind Narayanan is an assistant professor of computer science at Princeton University. Contact him at arvindn@cs.princeton.edu.