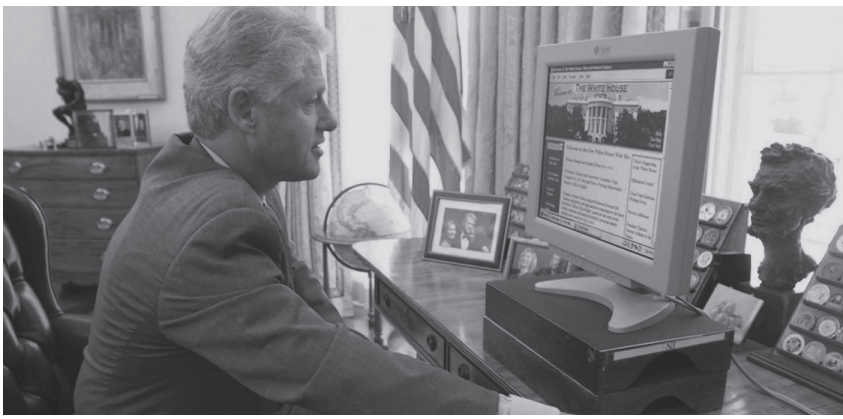
SURVIVAL OF THE



In January 1993, as then-President Elect Clinton was preparing to take office, a now-familiar Pennsylvania Avenue nemesis reared its ugly head: the email scandal. A young, exuberant presence during the campaign, Clinton's administration promised to inaugurate a new era for the White House. Technology would be centrally implicated in this new phase: the Clinton Administration would be the first to have its own website, the first to use email to communicate with the public. But though the White House didn't start using the internet in earnest until 1992, White House staffers had been using email to communicate internally since the Reagan era. And the Bush Administration did not want to leave records of its emails on computers that would be used by Clinton staffers.

Judge Charles B. Richey issued a restraining order preventing the Bush White House from destroying its records, shooting down a memo from the President's counsel saying they had the authority to do so. White House staffers framed the issue as a problem of resources: they needed to open up hard drive space for the new administration's files on White House computers. But it was quickly dismissed by Richey, who said, "As a practical matter, one does not need to know much about computers to know that saving this information is not going to bring the government to its knees" (Gerstenzang, 1993). Though the law prohibiting destruction of presidential records doesn't cover ephemera like scratch pads, informal notes, and visitor logs, by issuing the order Richey designated email a part of the public record of the administration (Bearman, 1994). "History is full of instances where the outgoing president has decided to erase, burn or destroy all or substantially all presidential or Executive Office of the President records before the end of his term," Judge Richey wrote in his forceful statement issuing the order (New York Times News Service, 1993).

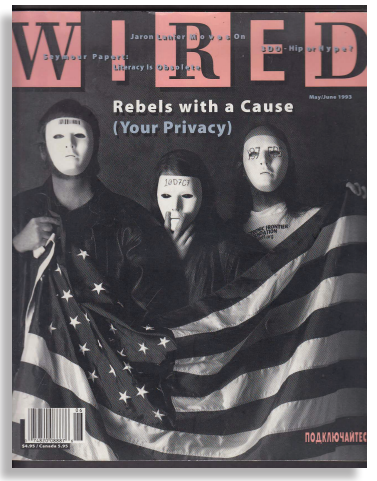
At its heart, the legal battle over email was about secrecy: Should the private communications of public officials be transparent to the public, and thus their political opponents? The conflict in the 1990s built upon a series of email scandals from previous administrations. As early as 1986, only a few years after the White House started using email, John Poindexter and Oliver North destroyed 5,000 email messages in an attempt to cover up the Iran-Contra scandal. The FBI found back-up copies and used them to piece together the affair; these emails became a key part of the evidence evaluated by the Tower Commission. In 1989, on President Reagan's last day in office, the National Security Archive filed a lawsuit to prevent the White House from deleting its email backup tapes. They were successful in doing so, and followed their suit with a case against President Bush toward the end of his administration. The Archive expanded its petition to the Court this time, asking them to formally rule that email falls within the jurisdiction of laws that require presidential administrations to hold on to their records (National Security Archive, 1995).

John Poindexter and Oliver North destroyed 5,000 email messages in an attempt to cover up the Iran-Contra scandal

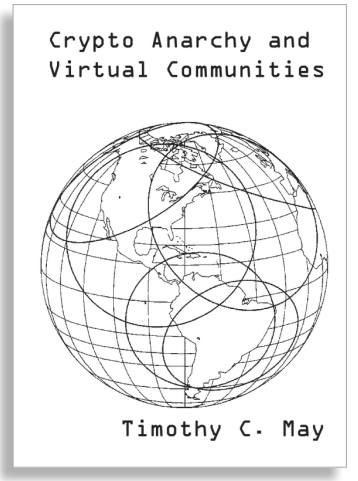
These early cases established that White House

Should we have privacy for the weak and transparency for the powerful? **Sarah Myers West** reminds us that we've been agonizing over this question since at least the 1990s, when the cypherpunks first started discussing it.

CRYPTIC



THE CYPHERPUNKS
Wired Magazine, May/June 1993.



CRYPTO ANARCHY AND VIRTUAL COMMUNITIES
Tim May's classic manifesto from 1994

emails generally fall within the bounds of public records laws. But the leaks, hacks, and scandals that marred the 2016 presidential elections suggest the underlying debate over the function of secrecy within a democratic government is ongoing. The elections raised many important questions about state secrecy: Should cabinet officials handling sensitive information be allowed to use private servers for their emails? Should the FBI announce when a presidential candidate is under investigation days before an election? How do we make sense of the practices of strategic leaking that are endemic to Beltway politics?

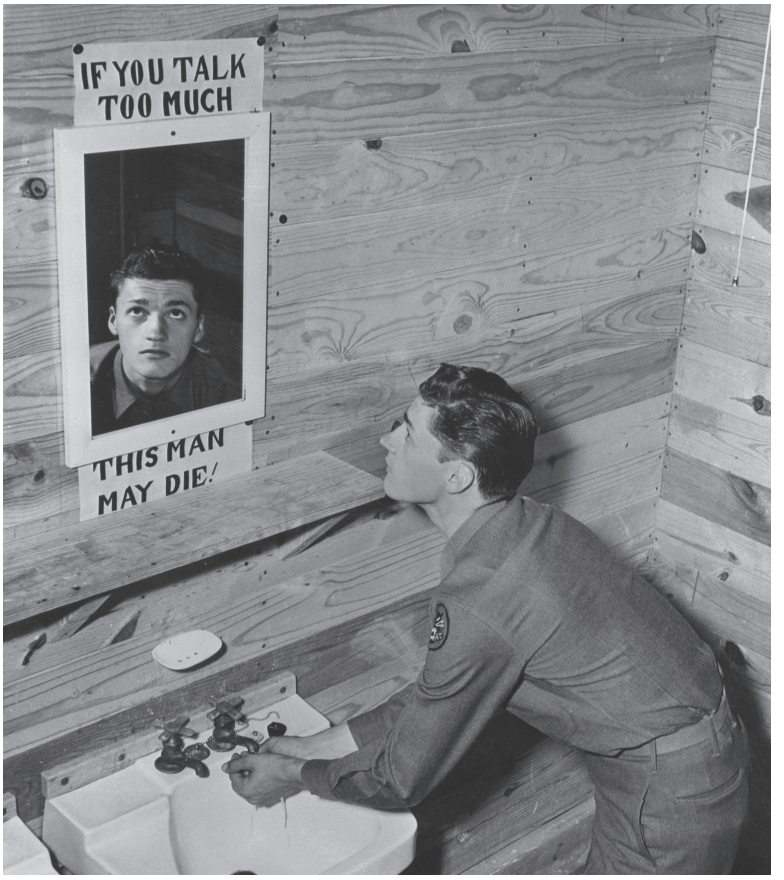
One of the leaks in particular has persistently remained at the center of the post-election debate: the penetration of the Democratic National Committee's (DNC) server by the hacker Guccifer 2.0, leading to the release of the DNC emails through WikiLeaks The DNC hack made visible the inner workings of a political party, raising questions about whether its secret machinations are compatible with the tenets of liberal democracy. At first, the leak seemed to force accountability within the Democratic Party for how it selects presidential candidates. But the months following have led to murkier questions over the true identity of the leaker and possible motivations behind the hack. As intelligence officials, congressional leaders, and journalists grapple with the fallout, the public is left grasping for a clearer view of what really transpired. Rather than making the secrets of government transparent and legible, in the end the DNC leak rendered them all the more opaque.

The "cypherpunks" sought to bring into being a world in which it would be possible to share and spread information about government activities while remaining secret

These questions about transparency and secrecy were central to the workings of a group of technologists in the early 1990s, and perhaps by looking at their debates we might make sense of our current situation.

The "cypherpunks," as they called themselves, sought to bring into being a world in which it would be possible to share and spread information about government activities while remaining secret, using public key encryption to verify their authenticity while protecting the identity of the leaker.

Debates among the cypherpunks during the Bush email scandal suggests this group of technologists was at the vanguard of thinking through the challenges of government secrecy. Though they don't reach any firm conclusions—and in fact differed considerably



TWO IMAGES OF HEROIC SILENCE
Left: Ollie North Shreds for America (provenance unknown); Right: "If you talk too much, this man may die." U.S. Office of War Information, 1943.

in opinions on which mechanisms for transparency would be preferable—at the advent of the White House's adoption of the internet the cypherpunks were already teasing out the nuances of the implications of networked technologies for the proper functioning of government. These nuances prefigure many of the tensions that reached a climax during the 2016 elections as a result of the DNC hack.

PRIVACY FOR THE WEAK, TRANSPARENCY FOR THE POWERFUL

In his *Crypto Anarchist Manifesto*, Timothy C. May, cofounder of the cypherpunks, remarked, "Computer technology is on the verge of providing the ability for individuals and groups to interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other.... These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation" (May 1992). Reacting to repeated attempts by state officials throughout the 1970s and 1980s to mask the inner workings of government—including those of the officials involved in the Iran-Contra scandal—May envisaged the development of a trade in national secrets, making it possible for whistleblowers to uncover corruption in government without risking harm to their physical selves.

May and other cypherpunks were inspired by texts like the 1985 science fiction novel *Ender's Game* by Orson Scott Card. In the book, two children post political essays anonymously to a global communication system under the pseudonyms Demosthenes and Locke, winning over policy experts and ascending to the world stage despite their youth. Anonymity enabled them to overcome the disparities in power and reputation accorded to their age: it leveled the playing field such that arguments were judged based on the content of their information rather than by the reputation of the speaker. May's vision builds upon this by seeking to establish a market in information separated from its institutional context. In so doing, May thought anonymous leaks could check the power of institutions like governments and corporations, redistributing it back to individuals.

Though Card's vision is very nearly an embodiment of Habermasian discourse, May's interpretation is more akin to a capitalist marketplace of ideas than a rationalized public sphere. "Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put

"The burden should not be on individuals to constantly be open to scrutiny to demonstrate their innocence"

into words and pictures," he said, leaving it up to the invisible hand of the market to define the value of that material (May 1992).

May extended these principles to the debate over White House emails. In an email to the cypherpunk listserv about the Bush administration case, he declared, "Individuals, corporations, clubs, and perhaps even government agencies should have the right to secure and private communications. The only caveat with the "perhaps" for the government is that it, in theory, belongs to 'us'" (Cypherpunk listserv, January 21, 1993). Though this statement is suggestive of some sort of carve-out for transparency in his philosophy for encryption, he quickly closed up that loophole: "I find it unsettling when people of one political party are screaming for access to the private diaries and papers of members of the other party. Citing Ollie North's crimes is no excuse" (Cypherpunk listserv, January 21, 1993). The vision May has articulated across these texts is suggestive of a philosophy not of mandated transparency, but of a marketplace of secrets, one in which the onus is on the secret-holder to maintain their own privacy through the use of encryption, and woe to those who wield it ineffectively.

Other cypherpunks proffered different views, however, raising a number of caveats in their discussion of the Bush emails that tease out nuances in the debate over government secrecy or transparency. Most turned to principles of liberal democracy and the concept of the social contract as justifications for a constraint on government secrecy: though institutions (individuals, groups of individuals, and companies) should have the right to private communication, they argued, those who act upon the consent of the governed must have some degree of transparency to ensure they stay accountable to the public.

As Eric Fogleman put it in a post on the Cypherpunk listserv, a mailing list through which the network of technologists communicated, "The right of government employees to private communication is limited by one important factor: many of these individuals are empowered to use force against citizens, and they responsible [sic] for justifying the use of this force.... Anyone given this kind of power has a heavy burden of proof and had better be able to prove beyond a shadow of doubt that their actions are justified. The burden should not be on individuals to constantly be open to scrutiny to demonstrate their innocence, but on those with the power to suspend individual rights" (Cypherpunk listserv, January 21, 1993). Fogleman's statement is akin to an early version of a maxim frequently stated by fellow cypherpunk Julian Assange: "Privacy for the weak, transparency for the powerful."

Many cypherpunks seemed to agree with this view but, as later emails suggest, at this point in time these cypherpunks' views fit within democratic frameworks of accountability rather than the kind of radical transparency Assange later espoused. Few cypherpunks at that moment built upon May's expressed vision for a stateless market in the trade of secrets. Responding to May's email, Dave Deltorto wrote that though Oliver North should have access to strong cryptography, he should be required to open his files if under criminal investigation. Deltorto later elaborated on this argument, saying that while documents produced by public officials on public time and in pursuit of public policy should be subject to scrutiny, their private communications on their own time should be excluded from this rule. He added, "HOWEVER, if such persons then turn around and abuse this freedom by abusing the public trust in those contexts (i.e., if Ollie North started communicating with NSA officials through CompuServe to order illegal shipments of money to CIA agents in Peruvian cocaine cartels), they should, by virtue of their positions of public trust be subject to the same (presumably high) levels of scrutiny as they are now—Congressional, OMB, GSA, FBI investigations, etc." (Cypherpunk listserv, January 21, 1993). Deltorto's argument relies upon the existence of government institutions to ensure officials act ethically, reforming from within rather than from without.

Or, as a cypherpunk going by the handle Lefty put it, "A *private* institution should have a right to *private* communications. The White House is *not* a *private* institution" (Cypherpunk listserv, January 22, 1993).

SURVIVAL OF THE CRYPTIC

May later elaborated on his vision in a post to the Cypherpunk listserv titled "Introduction to BlackNet." "BlackNet is in the business of buying, selling, trading and otherwise dealing with *information* in all its many forms," May said. "We buy and sell information using public key cryptosystems with essentially perfect security for our customers. Unless you tell us who you are (please don't!) or inadvertently reveal information which provides clues, we have no way of identifying you, nor you us" (Cypherpunk listserv, August 17, 1993).

The concept of the BlackNet was particularly amenable to a trade in state secrets, encouraging whistleblowers in government to adopt anonymity to render government more transparent through strategic leaks. Moreover, it would create an impetus for government officials to think about the protection of their privacy: "BlackNet believes it is solely the responsibility of a secret holder to keep that secret—not the responsibility of the State, or of us, or of anyone else who may come into possession of that secret. If a secret's worth having, it's worth protecting," May wrote. Technical savvy thus becomes both a means of facilitating transparency and a precondition for secrecy, a Machiavellian kind of survival of the cryptic.

The DNC leaks are in many respects a realization of May's ideas: the DNC hack demonstrated in stark relief the consequences of public officials' ignorance about their digital security. And in a sense, the organization WikiLeaks, which aided in the distribution of the DNC emails, is an embodied version of the BlackNet, with the notable difference that it doesn't operate purely on market logic. WikiLeaks' choice to act strategically in the timing of the emails' release resulted in an outcome that ran counter to May's expressed intentions:

the leaks asserted the dominance of geopolitical power rather than subverting it. The fingerprints of state-linked teams of hackers, not individual vigilantes, appear to be behind the hacks, which fit into a campaign of disinformation intended to sway the results of the election. The outcome was a diminution of individual agency, rather than its enhancement: a far cry from the vision May outlined in his manifesto.

SECRETS AND THE STATE

In "Sociology of Secrecy and of Secret Societies" (1906), Georg Simmel anticipated the morass that could surround government secrecy: "Secrecy secures, so to speak, the possibility of a second world alongside of the obvious world, and the latter is most strenuously affected by the former" (Simmel 1906: 462). Secrecy conveys on the secret-holder an exceptional position, he said, because of the fallacy that everything secret is somehow essential and significant. "Just as the moment of the disappearance of an object brings out the feeling of its value in the most intense degree," he said (Simmel 1906: 465), the revelation of secret knowledge can convey a sense of importance that may be outsized compared with the content of the information itself, a dynamic leveraged by the strategic use of leaks by actors seeking to sway the results of the election.

Simmel was adamant that in and of itself, secrecy "has nothing to do with the moral valuations of its contents" (1906: 462); it can be used by the benevolent to embrace their highest virtues, even as it is used by the malevolent to hide the darkest of evil acts. But he predicted that too much secrecy would make modern life intolerable: the realm of conspiracy, where truth could not be separated from fiction with any kind of objectivity, would be an undesirable state for any society to be in. As such, democracies are bound to regard transparency as a favorable condition, Simmel argued, following from the idea that every citizen is responsible for informing themselves about their government as a precondition for participating in it.

A decade before the formation of WikiLeaks and two decades before the DNC hack, the cypherpunks were already putting Simmel's sociological predictions to the test, anticipating how government secrecy and transparency would be transformed in a networked age. Despite their differences, the cypherpunks shared a vision of the redistribution of power through technology away from institutions and back to individuals.

The DNC leaks make clear that this vision has not been realized just yet: the strategic revelation of government information made the workings of political officials more opaque, rather than legible to the public. Both the hacks by Guccifer 2.0 *and* strategic leaks by government officials contributed to this opacity. This is an indication of the limits of transparency: while it remains a favorable condition for democracy, whether or not it will effectively aid the public in democratic deliberation depends very much upon by whom and for whom transparency is working. ■

SARAH MYERS WEST *is a PhD Candidate and the Wallis Annenberg Graduate Research Fellow at the USC Annenberg School for Communication and Journalism.*

BIBLIOGRAPHY

Bearman, D. (1994). "The Implications of *Armstrong v. the Executive Office of the President* for the Archival Management of Electronic Records." In *Electronic Evidence: Strategies for Managing Records in Contemporary Organizations*, (pp 118-144). Pittsburgh, PA: Archives & Museum Informatics.

National Security Archive. (1995). "White House E-mail". *National Security Archive*, November 22. http://nsarchive.gwu.edu/white_house_email/#LIST

Gerstenzang, J. (1993). "White House Told to Copy Records: Archives: In Fight over Computer Files, Appellate Panel Wants Bush's Staff to Back Up Notes and Memos before Erasing Anything. *Los Angeles Times*, January 16. http://articles.latimes.com/1993-01-16/news/mn-1353_1_white-house

May, Timothy. C. (1992). "The Crypto Anarchist Manifesto." *Cypherpunk Mailing List*. http://www.activism.net/cypherpunk/crypto-anarchy.html

New York Times News Service. (1992). "Administration Aides May Destroy Telephone Logs, Counsel Maintains." *The Baltimore Sun*, November 21. http://articles.baltimoresun.com/1992-11-21/news/1992326024_1_bush-white-white-house-telephone-logs

Simmel, Georg. (1906). "The Sociology of Secrecy and of Secret Societies." *American Journal of Sociology* 11(4):441-498.

Young, John. (2013). "Cypherpunks Archive 1992-1998." *cpunks.org*, September 6. https://lists.cpunks.org/pipermail/cypherpunks/2013-September/000741.html