Half-lives of hackers

Re: Risotto

From:john.podesta@gmail.com
To: peter_huffman@yahoo.com
Date: 2015-09-19 02:50
Subject: Re: Risotto

Yes and no
Yes it with absorb the liquid, but no that's not what you want to do. The slower add process and stirring causes the rice to give up it's starch which gives the risotto it's creamy consistency. You won't get that if you dump all that liquid at once.

and the shelf life of hacks

What is the speed of hacking? **Luca Follis** and **Adam Fish** explore the temporality of hacking and leaking in the cases of Snowden, the DNC leaks and the Lauri Love case.

FAST

Hackers helped Donald Trump win the 2016 U.S. election. It wasn't so much the content the hackers released about Hillary Clinton to the public through WikiLeaks; instead, it was the air of suspicion they created that lead to her undoing: the Secretary of State could be and was hacked. That became Clinton's problem, not what she and her colleagues wrote. Who had time to read the 19,252 emails from the Democratic National Committee (DNC) leak that WikiLeaks released four months before the election or the 20,000-plus emails from John Podesta—White House chief of staff and chairman of Clinton's US presidential campaign—published a month before the November 8 election? Muckrakers barely had time to conduct keyword searches in WikiLeaks's archives. The sheer size and breadth of the material made analysis difficult. Big data smothered interpretation. *Langue* Trumped *parole*.

Whether a slow and insistent "leak" or a cataclysmic data "dump," the pace, frequency, and size of the hack matters. Blindingly fast and impenetrably large, the political impact of the hack is potentially larger than the content contained within. Here we plot the temporalities of three hacks ranging from the fast to the slow to the still: we describe the excesses in volume and speed in the Clinton case, the slow journalism of the Snowden/Greenwald collaboration, and the non-leaked hack of Lauri Love, an Occupy and Anonymous hacktivist scheduled for extradition to the United States for allegedly hacking military and banking institutions but not releasing any material.

Some of the material in the DNC and Podesta leaks did receive attention, whether it was due or not. For example, Edgar Welch was inspired by blogged conspiracy interpretations concerning the reoccurrence of the worrisome term "pizza" in the emails and their obvious connection to a Clinton child sex slave dungeon located in a Washington, DC, pizzeria. So on December 4, 2016, carrying a shotgun, assault rifle, and .38 revolver, Welch went to the Comet Ping Pong restaurant to search, in his report to police, "for evidence of hidden rooms or tunnels, or child sex-trafficking of any kind" (Jarrett 2016). Finding none, he shot up the place with his AR-15 rifle and was arrested on federal charges for this mission on behalf of what came to be known as "fake news." Facebook CEO Mark Zuckerberg has emerged with a seven-point plan to tame "fake news" on his website including the typical crowd-sourced self-regulation and self-reporting or flagging (Jamieson and Solon 2016). We can't wait to get officially illicit along with our Facebook-verified news and hacks.

While thankfully no diner at Comet lost their life because of this poor hermeneutical reading of hacked leaks, somebody likely did lose the U.S. presidency because of it. "Spirit cooking" was a trending term days before the 2016 U.S. presidential election. In an email from performance artist Marina Abramović, Podesta was invited to dinner with the line, "I am so looking forward to the Spirit Cooking at my place" (Lee 2016; Podesta did not respond to this invitation). The alt-right seized upon this term as an oblique reference to satanic rituals involving human sacrifice, with

DIVER SIGNALS COURTESY OF WIKIMEDIA COMMONS

Clinton seated at head of the occultic new world order (Ohlheiser 2016). These are some of the few stories to come from the trove. Otherwise, much of it is boring, trivial, and gossipy, or requiring the skilled interpretive acrobatics of the best conspiracy theorists.

Some of the material revealed—Clinton's staff emails colluding with the DNC to dispose of Democratic challenger Bernie Sanders, her Wall Street speeches, and the forms of "pay-to-play" access given by the Clinton Foundation to the global elite—does present damning evidence. Yet it wasn't the content, we argue, but the impenetrable volume and the breakneck pace of the leaks that cursed Clinton and puzzled journalists. Whatever legitimate political harm was created by the disclosures was not a result of analysis, attribution, or even denial.

The present world of hacks and leaks is front-loaded. It is overwhelmingly determined by the volume and pacing of the disclosures, a fact that can substantially eclipse the revelatory (and factual) nature of the material itself. It is true that economic and demographic reasons are more likely contenders than an email scandal for why Clinton lost to an unprepared, platformless, tax-dodging, racist, bankruptcy-prone, misogynistic, fact-phobic, former reality television star. But it certainly didn't help. Her quandary provides a window into a new politics of suspicion that forms at the intersection of volume, velocity, and disclosure, factors that eclipse revelation, attribution, and denial, which are the stickier subjects of scandal. Excess and speed, the sheer volume of the hacked materials paired with the velocity with which the content appeared on contraband websites—in user-friendly boolean searchable form, no less—are the quintessential marks of the hacktivist today.

Velocity and volume combine powerfully and call to mind Paul Virilio's (1977) writings on the impact of technologically hastened politics. His term "dromology" refers to the inner logic of speed and the moving object's tendency to dominate slower rivals. It is an apt way to think about the current state of leaks: fast volumes dominate the headlines and overtake slow journalism. The present moment in hacktivist history is marked by an excess of information exploding centrifugally outward against both left and right political ideologies. Clinton was a victim of the excess dromology of this election cycle. But not all hacks need to follow this pace and fill public space in this manner. There remains a time and space for revelation.

SLOW

On June 6, 2013, Glenn Greenwald published a story in *The Guardian* based upon a top-secret court order requiring Verizon (a major U.S. telecom company) to provide the National Security Agency (NSA) with information on all telephone calls in its systems within the United States and between the United States and other countries. The following day, *The Washington Post* and *The Guardian* published the first stories detailing the NSA's bulk domestic surveillance program PRISM along with four internal PowerPoint presentation slides from the whistleblower and former NSA employee Edward Snowden. Snowden's disclosures were parsimonious and carefully chosen, accompanied by careful and contextual reporting, and their overall sequencing was staggered over the course of multiple years (Greenwald 2015).

Indeed, apart from the tremendous political impact of his revelations, what remains striking today is the fact that the published and publicly disclosed documents represent a very small proportion of the full Snowden trove. The archive that Snowden shared with news outlets contained about 50,000 documents, of which approximately 7,300 have been released since 2013. Further, although there is debate about the total number of sensitive documents he downloaded from the NSA, conservative estimates put the figure at 1.5 million (Kloc 2014).

Contrast this figure with the 20,000 Democratic National Committee emails, 891 documents, and 175 spreadsheets released by WikiLeaks on July 22, 2016, just days before the Democratic National Convention was held in Philadelphia (July 25–28). The data hacking is notable because of its timing, sheer volume, and indiscriminate character: John Podesta's risotto tips absurdly sit alongside evidence of strong anti–Bernie

Sanders bias among staffers. And just days after the leaks, in the midst of the national convention, DNC Chairwoman Debbie Wasserman Schultz resigned. The following month DNC CEO Amy Dacey, CFO Brad Marshall, and communications director Luis Miranda all announced their intention to leave the DNC (Tau and Nicolas 2016).

Clearly the leaking of the Snowden and DNC documents was timed for maximum impact. Although the former sought to influence then-current events, the full impact of the disclosures is oriented towards the *longue durée* and the extensive digital archive of American global panopticism that will be preserved in posterity. The DNC leaks, on the other hand, were timed for immediate, disruptive, and destabilizing force: that is, their form (the fact they existed and their sheer size) had more impact than their actual content. Further, in contrast to the selective and parsimonious character of the Snowden disclosures (and some prior WikiLeaks releases), the DNC files were published all at once and with no apparent curation.

The difference between these two "leaks" or disclosures is also informative with respect to the shifting tactical uses of identity and attribution. Snowden's character and motivation became integral components of the story, providing an anchor for the leaked material that also gave it salience and immanence, and vouched for its authenticity. In contrast, everything known about the DNC hacks seems designed to confound, frustrate, and work against the intuitive alignment between legitimate political activism, information transparency, and whistleblowing. Initially, the hack was attributed to two different Russian intelligence adversaries, Cozy Bear and Fancy Bear. And while six cybersecurity firms and two newspapers agreed that the level of sophistication—and a few self-incriminating mistakes—indicated a Russian state-level hack, other names and motives soon arose. The first pseudonym to step forward was Guccifer 2.0, a reference to the 1.0 Guccifer, a Romanian hacker extradited to the United States and recently sentenced to 52 months in federal prison. Guccifer 2.0 claimed to be a hacktivist colleague of the original Guccifer until questions concerning his fluency in Romanian and his connection with Russia surfaced (Goodin 2016).

That WikiLeaks released the DNC emails certainly did not help clarify matters, and Julian Assange's sloppy remarks on Dutch TV identifying the leaker as recently murdered DNC staffer Seth Rich only generated further ambiguity (Stahl 2016). Thus far, the DNC hacks have been linked to the Russian state, Romanian hackers, a dead DNC staffer, and—as one former NSA analyst and counterintelligence officer for the Navy claimed—the NSA itself (Schindler 2016). The DNC hacks provide a glimpse into one facet of the shifting tactical array employed by state-based forms of hacking in which the political tropes, themes, and expectations we have come to associate with hacktivist and whistleblowing disclosures (including the factual authenticity of the material itself) are hijacked for anti-political and disruptive effect.

INERT

Hacks may be small or large; they may contain influential evidence or not. Some hacks we don't know about because they are never made public. We know of their existence through hearsay, rumor, or acts of partial transparency. We know of the form, but not the content; the deed but not its result. The case of Occupy activist and alleged Anonymous associate Lauri Love is a case in point. In July 2016, Westminster Magistrates Court ruled that the United Kingdom would extradite the Finnish-Welsh hacker to the United States to face computer fraud charges in three federal jurisdictions. Little is known about the accusations actually leveled against him. It's not just that the rules of extradition prevent the examination of Love's alleged criminal activities but also that the content Love is charged with exfiltrating from the United States was never publicly released. This is the leak that never happened, and Love faces 100 years in jail for it.

Love's case is connected with the suicide of internet freedom activist Aaron Swartz on January 25, 2013, and the political action that followed his death. Two weeks later, Anonymous initiated Operation Last Resort, which included the hijacking of a Massachusetts

Institute of Technology (MIT) website to create a Swartz tribute as well as the usurping of the U.S. Sentencing Commission website (ussc.gov) and a website of the Department of Justice (Blue 2013). The only leak associated with Operation Last Resort is the release of the 4,000 banking executives' names on February 4, 2013, which contained no information of political significance (Robertson 2013). This hack was a spectacle without the substance.

Associated with the action, Anonymous claimed to have distributed encrypted government files pertaining to U.S. Supreme Court Justices and threatened to release the decryption keys if the government did not reform the draconian laws they believed led to the death of Swartz. In press releases and videos, Anonymous called these decryption files, each referencing a U.S. Supreme Court Justice, "warheads," for example "Scalia.warhead1." Why weren't the keys released, and what does their absence mean for the study of the political impact and consequences of hacking?

In contrast to Snowden and the DNC hacks, the temporality of Love's alleged hack does not follow the trajectory and pace of the 24-hour news cycle but is oriented to the slow temporalities of the criminal justice state. On October 23, 2013, the first of three U.S. court indictments against Love were filed. Two days later he was arrested and a search warrant was served on his parents' house. Nine months separated the initiation of Operation Last Resort and Love's arrest. On July 3, 2014, Love was released on bail, his passports were returned, and the Crown Prosecution Service declined to prosecute for lack of evidence. Almost one year later (July 15, 2015), Love was arrested again, this time by the Metropolitan Police's extradition unit for the outstanding U.S. indictments connected with Operation Last Resort, which include hacking into the Federal Reserve, the U.S. Army, NASA, and the Missile Defense Agency. From June to July 2016, Love appeared in court challenging the extradition request and was denied on September 16, 2016, when Judge Tempia ruled in favor of extradition. Love has an appeal, but it is likely that he will eventually face his accusers in the United States and be sentenced to significant time in prison.

The case provides an important counterpoint to Snowden and the DNC hacks. This is the leak that never happened. Its temporality was interrupted and hijacked by a criminal justice process that has and will continue to control the tempo, volume, and content of material that will appear in the public record with respect to Operation Last Resort (Fish, forthcoming). It is likely that what will be revealed in Love's criminal trial(s) will be scrubbed of its impact and separated from the political events that gave it relevance by the slow time of courtrooms and the veil of prosecutorial abstraction. In this sense, the inertia that surrounds the case also crystallizes the stakes involved: Love's ability to frame the hack as an instance of political activism or in terms of public interest claims concerning the content of the material he exfiltrated is vitiated by the very real threat of self-incrimination (Fish and Follis 2016). In the absence of such an account, the courtroom becomes a space for the deployment of a very particular technology of truth. Who is Lauri Love? What are his motives? How grave are his actions? Is he an activist, a terrorist, or a foreign agent? These questions swirl around the case and assert themselves in the interpretive vacuum generated by his criminal defense.

Operation Last Resort, much like the Snowden disclosures and the DNC hacks, points to the emergence of a powerful "hermeneutics of suspicion" (Ricoeur 1970) where the deeper (and perhaps more authentic) meaning that sits behind text and event, between actor and act, oscillates unpredictably under the force of multiple, fractious interpretations delivered contemporaneously. The variegated publics that are its targets have grown increasingly insular, wary of expert claims, and skeptical of the facts that support them. In response, a new counter-critical common sense informs their reading of political and world events, a reading both determined by and filtered through a dromological news cycle saturated with leaks and data dumps.

BIBLIOGRAPHY

Ashok, India. 2016. "Weebly Confirms Over 40 Million Users, Foursquare Accounts Are Also Exposed." *International Business Times*, October 21. Available at link

Blue, Violet. 2013. "Anonymous hacks US Sentencing Commission, distributes files." *ZDnet*, January 26. Available at link.

Fish, Adam R. forthcoming. "Scalia.warhead1: Securitization Discourses in Hacktivist Video." In *Visual Security Studies: Sights and Spectacles of Insecurity and War*, edited by J. Vuori and R. Saugmann. Abingdon-on-Thames, UK: Routledge.

Fish, Adam R., and L. Follis. 2016. "Gagged and Doxed: Hacktivism's Self-Incrimination Complex." *International Journal of Communication* 10:3281–3300.

Goodin, Dan. 2016. "'Guccifer' leak of DNC Trump Research has a Russian's fingerprints on it." *Ars Technica*, June 16. Available at link.

Greenberg, Andy. 2016. "Hack Brief: Yahoo Breach Hits Half a Billion Users." *Wired*, September. Available at link.

Greenwald, Glenn. 2015. *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State*. New York: Picador.

Jamieson, Amber, and Olivia Solon. 2016. "Facebook to begin flagging fake news in response to mounting criticism." *The Guardian*, December 15. Available at link.

Jarrett, Laura. 2016. "'Pizzagate' shooting suspect facing new federal charges." *CNN*, December 13. Available at link.

Kloc, Joe. 2014. "How Much Did Snowden Really Take? Not Even the NSA Really Knows." *Newsweek*, June 9. Available at link.

HACK HOROLOGY

On the top shelf of a dusty Oxbridge bookshelf, we can already see the 2017 *Oxford English Dictionary* making room in itself for a "fake news" sequel to its 2016 word of the year, "post-truth." The volumetric and expedient hack contributes to this erosion of facts creating an aura of ambiguous "truthiness," the Merriam-Webster 2006 word of the year. As speculation and conspiracy increase, the English dictionaries—like the hegemonic public sphere—are reflecting the erosion of consensual reality, and logical democratic consensus is a victim.

Political hacks today come in the context of pervasive data insecurity and systemic cyber vulnerability. Whether it's news that many major companies (e.g., LinkedIn, Dropbox, Tumblr, Yahoo, Foursquare, Weebly) have recently suffered large-scale data breaches or the dramatic outages caused by the recent global distributed denial of service (DDoS; when a hacker makes a network unavailable to its users) attack on internet switchboard company Dyn, it seems as if everything and everyone in our media-saturated societies is now potentially vulnerable, including our sense of reality (Ashok 2016; Greenberg 2016).

The temporality and volume of leaks influences their public reception, meaning, and impact. The primacy of these two factors displaces and distorts some of the categorical, normative, and political inventory we traditionally use to make sense of the motives of hackers/leakers and the importance of their disclosures. In other words, speed and volume displace and distort the most analytically important category of all: revelation.

One conventional way of thinking about political hacks and leaks (as opposed to breaches) involves their *revelatory* intent. The strength and impact of a leak or data dump are usually tied to the extraordinary character of the material contained in the disclosure. An influential leak is factual; it provides information or documents that offer incontrovertible legal-grade proof of a whistleblower's or leaker's claims about the state of reality. Such leaks can usually weather official denials and evasions. Indeed, in cases of serious criminal activity or malfeasance, leaks might prompt governmental action through investigations and/or prosecutions.

The situation we describe here is one in which the extraordinary has become commonplace and where radical information transparency is ubiquitously, indiscriminately, and summarily applied. One danger here is that the sheer volume, speed, and frequency of disclosures is greatly outpacing our capacity to separate politically salient or criminally significant acts and facts from the ambient digital noise they come bundled with. On the one hand, this clearly points to the need to better align tactics of revelation and disclosure with questions of timing and scale.

Yet in a deeper way, it also seems to threaten the capacity of digital technology and the web to serve the wider project of critique and dissent because the dromology of the data dump feeds into and strengthens already existent power asymmetries. We have already noted how the DNC hacks illustrate the increasingly common appropriation of hacktivist tropes and forms by state power, thereby coopting the tactics of the weak into stratagems of power. In a world where the effect or impact of a leak is divorced from the content it contains, it becomes possible (even inevitable) that faux leaks and fake news become yet another tool in the arsenal of states. ■

LUCA FOLLIS *is a political sociologist and Lecturer in the Law Department at Lancaster University; his work focuses on the intersection of law, the state and resistance.* **ADAM FISH** *is an anthropologist and Senior Lecturer in the Sociology Department at Lancaster University where he researches digital industries and digital activism. He is the author of the book* Techoliberalism *(Palgrave Macmillan) and co-author of* After the Internet *(Polity).*

Lee, Benjamin. 2016. "Marina Abramović mention in Podesta emails sparks accusations of satanism." *The Guardian,* November 4. Available at link.

Ohlheiser, Abby. 2016. "No, John Podesta didn't drink bodily fluids at a secret Satanist dinner." *The Washington Post*, November 4. Available at link.

Ricoeur, Paul. 1970. *Freud and Philosophy: An Essay on Interpretation.* New Haven, CT: Yale University Press.

Robertson, Adi. 2013. "Anonymous Posts banking industrial data dump in ongoing Aaron Swartz protest." *The Verge*, February 4. Available at link.

Schindler, John. 2016. Did the NSA Try to Destroy Hillary Clinton, *Observer*, August 8. Available at link

Stahl, Jeremy. 2016. "WikiLeaks is Fanning a Conspiracy Theory that Hillary Murdered a DNC staffer." *Slate*, August 9. Available at link

Tau, Bryan, and Peter Nicholas. 2016. "Three More Democratic Officials Resign in the Wake of Email Leak." *Wall Street Journal,* August 2. Available at link

Virilio, P. 1977. *Speed & Politics: An Essay on Dromology*. New York: Semiotext(e).


Se toco â su Original
el dia 2o de Mayo de 1749 a.s