Why Clouds Give Me a Case of the Vapors

Hal Berghel, *University of Nevada, Las Vegas*

Recently, Apple admitted that revealing photos of celebrities had been released on the Internet due to security breaches associated with its iCloud and Find My iPhone systems.

According to Apple, " … certain celebrity accounts were compromised by a very targeted attack on user names, passwords, and security questions."[1] Didn't we cover defensive privacy tactics in my January column?[2] Color me dazed and confused! Hacking in cyberspace? Nothing like that's ever happened before. (I've got another heads-up for you iPhone users—Siri talks about you behind your back. I'm just sayin'.)

In my personal life I build trusted relationships one tax-avoiding, jurisdiction-shopping, multinational corporation at a time. Show me a company that engages in labor arbitraging and offshore production in third-world countries paying starvation wages[3] and that avoids taxes through shadow companies in Ireland (Apple Operations International) so it can reap real profits in the US only to pay virtual taxes in invisible jurisdictions[4]—what *The New York Times* calls the "Double Irish with a Dutch Sandwich"[5]—and I'll show you a company that deserves my full faith and confidence. Passwords? Crypto keys? Security questions? Not needed. Oh, corporate giants, have your digital way with me!

INTO CLOUDS A LITTLE RAIN MUST FALL

According to popular lore, the concept of cloud computing dates back to the turn of the new millennium, when Amazon sought to capitalize on unused cycles during non–peak usage periods. *MIT Technology Review* traces the term *cloud computing* itself back to 1996, when a few Compaq Computer employees used it to describe the business opportunities arising from moving applications and data to the Web.[6] The *cloud* became the metaphor for the Internet. *Sump* might have been a better one—but I digress.

As Simson Garfinkel explained in the October 2011 issue of *MIT Technology Review,*[7] the cloud concept actually dates back much farther. According to Garfinkel, MIT Professor John McCarthy envisioned the organization of computing and networking resources as public utilities in a global resource-sharing environment in 1961. In turn, McCarthy's vision can be traced back to Vannevar Bush's notion of a memory extender, or memex, which he described in 1945 in *The Atlantic Monthly.*[8] Cloud's analog analogue traces back to antiquity—the concept behind a sharable public data repository dates as far back as the earliest libraries. What the current generation has added to the concept is a digital structure ensconced in a modern business model.

DIGITAL VAULTS, CRYPTS, AND OSSUARIES

I prefer to look at digital repositories as digital vaults, crypts, and ossuaries distinguished by content, purpose, and access. A generic online repository with real-time access is a digital vault (appropriate for data use). Digital crypts, as the name implies, are the final resting grounds for data—useful for static data at rest. Digital ossuaries occupy the middle ground of online storage for archival purposes (for example,

 Published by the IEEE Computer Society

nonstatic data at rest). These distinctions are important because they call for different business plans and security models; failure to appreciate them caused actress Jennifer Lawrence and model Kate Upton considerable discomfort.

Let's deal with digital crypts first. Like their namesakes under Paris and Rome, digital crypts house objects that are likely retained for archeological, forensic, or regulatory purposes, serving libraries, governments, businesses, and industry as backups and for compliance. In the normal course of events, they can rest quietly and undisturbed for long periods, have little currency, and might be stored offline in minimum-security settings when required. Old salt mines and deprecated missile emplacements would be good candidates for digital crypt locations. Hacks, malware, scams, phishing, and their cousins aren't big threats to crypts. This lowers the storage cost and simplifies the business model.

Next up the food chain are digital ossuaries. These serve as archives as well, but they must be online to be of maximal use. Examples include medical and accounting records, transaction histories, and the like. Repositories of entities covered by the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), and the Gramm-Leach-Bliley Act (GLB) would certainly qualify as ossuaries. I specifically mention HIPAA, SOX, and GLB because of their requirements for privacy and security controls, which are beyond those for crypts. This business plan requires a sophisticated storage network and infrastructure augmented with a carefully thought-through information security plan and implementation. Ossuaries might live quite comfortably on a proprietary local area network. In fact, that might be optimal in many cases.

Finally, we move to digital vaults—what most people associate with "the cloud." Here, anything is accessible in milliseconds from the Internet. They contain everything that customers choose to store there—from proprietary and classified information to Jennifer's and Kate's selfies. Because of this ad hoc intermixture of data, it's not always clear what's optimal from a business, security, or privacy policy standpoint. Therein lies the rub. Needless to say, digital vaults are found in dangerous network neighborhoods where denizens of digital derring-do might lurk behind every cloudlet. Think of this as the fog of war—cybermode.

There's far too much trust required in cloud services—they're the new millennium's digital faith-based initiative.

The digital vault metaphor serves to call your attention to the absence of standard safeguards normally associated with its physical counterpart. When we store things in our safety deposit boxes, bank vaults, or home safes, we experience the look and feel of physical security measures being taken to safeguard our possessions. How would you feel if you exchanged your briefcase full of family heirlooms for a mere promise of safekeeping from an unknown bank teller? For most of us that would be as unwelcome as flatulence in a spacesuit. We want to physically and personally verify the custodial transfer of our possessions—either by placing the goodies in our dual-keyed safety deposit box ourselves or witnessing their placement in a vault by a bank officer.

That's what's missing from modern cloud services. Overconfidence is our default state for Internet-based digital storage. We wouldn't accept unverifiable promises from our banks, and we probably shouldn't accept them from our cloud services either. Even vault ownership—as in each pod, rack, and container used in cloud systems—means little if we're unable to control access to it. There's far too much trust required in cloud services—they're the new millennium's digital faith-based initiative.

DIGITAL METEOROLOGY

I should emphasize that I take no position on the management of datacenters—I leave such matters to industry standards groups like the Uptime Institute (uptimeinstitute.com) and the Cloud Security Alliance (www.cloudsecurityalliance.org). My remarks are best taken philosophically: I think that it's prima facie obvious that you shouldn't entrust personal, proprietary, and sensitive information to third parties unless it's required by law or because other alternatives have proved impractical or unreasonable. I also challenge cloud services' cost-effectiveness. My hunch is that like major league sports franchises, cloud services are only economical when the cost of ownership is calculated to exclude negative externalities, moral hazards, and off-the-books expenses.

So why did public cloud services become popular? Certainly disaster avoidance and recovery figure prominently into their adoption. There are organizations that are too large to think of force majeure as an insurance issue, yet too small to manage the risks themselves. These organizations are typically labeled small to midsize businesses. There is an important niche market among SMBs for cloud services. Colocation (COLO) providers that promise reliable power, secure network access, cooling, redundancy, fire protection,

fault tolerance, physical security, and so forth enable contingency planning well beyond the capability of many customers. The major COLO providers like Equinix, Century Link, SunGard, AT&T, and the like seem to provide useful services for customers that can't or don't want to provide these services themselves.

However, cloud services are undergoing commodification. It's unclear to me how one would differentiate tier IV datacenter infrastructures in terms of mission-critical capabilities. So although there is a market for colocation providers, it isn't clear that there will be a market to support the number of colocation providers we now have for very much longer. In an era where even the Justice Department shies away from oligopolistic accusations, not to mention prosecutions, I would expect that a cycle or two of merger-and-acquisition (M&A) mania in the near future will drastically reduce the number of clouds in the digital sky. Such being the case, we'll likely end up with less competition, lessening of quality-control standards, and tighter-fisted economics as these phenomena seem to be an inevitable byproduct of M&A mania. Smaller customers will be the first to feel the loss of prophylaxis.

The inevitable cloud commodification will affect their *future* utility, value, and appeal. However, there are some other considerations that affect their *present* utility, value, and appeal. For one, there's considerable overlap between the cloud providers and the National Security Agency company "partners" identified in the Snowden PRISM slides (https://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29). In many cases these companies willingly shared customer information with the NSA without requiring a court order (http://arstechnica.com/information-technology/2014/06/a-year-after-snowden-internet-crypto-remains-spotty/). So just how confidence-inspiring is this corporate behavior?

My cloudtopsy reveals the cloud's four humors: early mortality, lack of constitutional safeguards in the US, possible ISP leakage and snooping, and VPNs that we can't trust. Think of these as modern cloud computing's toxic biles, phlegm, and bad blood!

THE CLOUD'S FOUR HUMORS

Even if you're confident in the *cloud* service, how confident are you in the ISP that serves as a conduit between your organization and the cloud? It should be noted that in many cases the recent gains in privacy protection, including SSL encryption of transiting data, were a direct result of the blowback that resulted from Snowden's disclosures (http://arstechnica.com/information-technology/2014/06/a-year-after-snowden-internet-crypto-remains-spotty) and not because of any customer-service concerns. But even at that, the Electronic Frontier Foundation's best practices still haven't been completely implemented (https://www.eff.org/encrypt-the-web-report). The point I'm making is that ISPs generally seem to favor reactive rather than proactive positions when it comes to protecting customer data.

Add to this the fact that federal courts have taken the position that the government, not the courts, has final say when it comes to requests for customer data. When the FBI demanded real-time access to select customer data on Lavabit's secure email servers, the only way to comply would be to give up all SSL keys, which meant providing real-time access to *all* customer communications, not just a select subset. I encourage you to learn about the FBI's policies and the current status of the Lavabit case. (For an overview, see http://blogs.findlaw.com/fourth_circuit/2014/01/today-is-lavabits-and-the-4th-1st-amendments-day-in-court.html and http://rt.com/usa/lavabit-contempt-affirmed-appeal-996). The most recent ruling from the US Court of Appeals, Fourth Circuit, is online at http://caselaw.findlaw.com/us-4th-circuit/1663658.html.

Remember that all US-based cloud storage providers are subject to US laws, specifically including the Patriot Act (https://epic.org/privacy/terrorism/hr3162.html) and its equally constitutionally unfriendly descendants (www.salon.com/2014/09/04/patriot_acts_absurd_new_spawn_just_when_you_thought_it_couldnt_get_any_worse). Although access to email usually requires a warrant (www.law.cornell.edu/uscode/text/18/2703), this might not be the case with cloud storage. You'd be well advised to create a new "cloud lawyer" position in your organization to interpret Title 18 language for you (www.law.cornell.edu/uscode/text/18/2703). And the time to do that is before you consider adopting any cloud service.

Finally, the VPN service providers you might use to encrypt the pipe between you and the cloud are subject to the same government intrusions as ISPs and cloud services. Cloud VPN provider CryptoSeal terminated its service in June 2014 for just this reason (http://arstechnica.com/information-technology/2013/10/cryptoseal-vpn-shuts-down-rather

-than-risk-nsa-demands-for-crypto-keys). Silent Circle shut down Silent Mail, its encrypted email service, for fear that the government might issue National Security Letters (NSLs) demanding metadata (http://techcrunch.com/2013/08/08/silent-circle-preemptively-shuts-down-encrypted-email-service-to-prevent-nsa-spying). Both providers saw the writing on the wall after Lavabit's experience (www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email).

Understand that NSLs arrive with a gag order and the prohibition of seeking counsel! Until peer-to-peer encryption based on ephemeral keys (or something like it) is deployed everywhere, mobile Internet access to any data repository is fraught with legal uncertainty. To its credit, Silent Circle did just that with its Silent Phone service (https://silentcircle.com/services), specifically encrypting traffic at the media layer because carriers and ISPs might not be trustworthy. As I write this, the FBI has requested changes in the federal rules of criminal procedure (http://justsecurity.org/wp-content/uploads/2014/09/proposed-amendment-rule-41.pdf) specifically to allow seizure of any target whose identity is concealed by technological means like Tor (http://hackread.com/fbi-will-hack-any-overseas-tor-vpn-user).

So there you have it. My cloudtopsy reveals the cloud's four humors: early mortality, lack of constitutional safeguards in the US, possible ISP leakage and snooping, and VPNs that we can't trust. Think of these as modern cloud computing's toxic biles, phlegm, and bad blood! And as with the medical humorism of old, when data concentration is the rule, any deficiency in one of these humors will produce a bad case of the network computing vapors. I'm confident that Hippocrates would be pleased with my analysis.

Cloud services remind me of distance education—not a bad idea if the focus is entirely on improving the overall customer (or student) experience. However, that's not the way it evolved. In the hands of nonscholar administrators, distance education became first and foremost an opportunity to grow revenue with minimal investment. Increasing the student's quality of experience went to the back of the budget bus. Similarly, I fear that the best interest of the customer—particularly in terms of protecting customer privacy—isn't the leading priority of cloud service providers. In any event, if you're considering the addition of clouds to your sky, be sure to lawyer up and think hybrid (www.businessnewsdaily.com/4427-cloud-computing-small-business.html), because being in the cloud might become your single greatest vulnerability.

RELATED RESOURCES

For an overview of cloud computing, see the NIST Cloud Computing Reference Architecture: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf.

References

1. B. Solomon, "Apple Admits Celebrity Photos Were Stolen in Targeted Hack," *Forbes*, 2 Sept. 2014; www.forbes.com/sites/briansolomon/2014/09/02/apple-admits-celebrity-photos-were-stolen-in-targeted-hack.
2. R. Cooper, "Inside Apple's Chinese 'Sweatshop' Factory Where Workers Are Paid Just £1.12 per Hour to Produce iPhones and iPads for the West," *Daily Mail*, 25 Jan. 2013; www.dailymail.co.uk/news/article-2103798/Revealed-Inside-Apples-Chinese-sweatshop-factory-workers-paid-just-1-12-hour.html.
3. T. Dickinson, "The Biggest Tax Scam Ever," *Rolling Stone*, 27 Aug. 2014; www.rollingstone.com/politics/news/the-biggest-tax-scam-ever-20140827.
4. C. Duhigg and D. Kocieniewski, "How Apple Sidesteps Billions in Taxes," *The New York Times*, 28 Apr. 2012; www.nytimes.com/2012/04/29/business/apples-tax-strategy-aims-at-low-tax-states-and-nations.html.
5. A. Relgalado, "Who Coined 'Cloud Computing'?," *MIT Technology Rev.*, 31 Oct. 2011; www.technologyreview.com/news/425970/who-coined-cloud-computing.
6. S. Garfinkel, "The Cloud Imperative," *MIT Technology Rev.*, 3 Oct. 2011; www.technologyreview.com/news/425623/the-cloud-imperative.
7. V. Bush, "As We May Think," *Atlantic Monthly*, 1 Jul. 1945; www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881.

Hal Berghel *is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.*