SECOND LOOK

Client Data, the Cloud and NSA Surveillance

by Pete Haskel

I've been speaking a lot lately about the ethics of putting client data on the Cloud. But the recently-disclosed National Security Administration (NSA) surveillance programs put a whole new slant on this issue.

"The Cloud" is shorthand for housing data, programs, security, or other computer or networks services on remote servers – outsourcing some or all aspects of computer functions.[1]

The debate over whether lawyers can ethically house client data on the cloud is heated and unsettled (not to mention unsettling). The ABA has collected relevant state ethics opinions.[2] State ethics opinions generally permit lawyers to use the cloud to store client data as long as the lawyer makes reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client (the Model Rules of Professional Responsibility formulation for attorney's level of care to protect confidential client information[3]) unless the client prohibits using the cloud.[4] In addition, many state ethics opinions add significant, sometimes onerous, and often ambiguous, cautions and mandates, such as requiring scrutiny of the cloud provider's terms of use for "enforceable"[5] contract provisions as to confidentiality and security,[6] making the lawyer keep abreast of relevant technology developments,[7] and/or consider enumerated factual and legal issues in engaging a cloud provider.[8] Even after making lawyers jump through such hoops several opinions caution to the effect that, "As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information. . . ."[9] In addition, the ABA in August 2012 amended a comment on the ABA rule on attorney competence that would require, that a lawyer's duty to keep up with changes in the law includes keeping abreast of changes in "the benefits and risks associated with relevant technology."[10]

But none of these cloud-centric ethics opinions detract from the fundamental principle that the attorney must use reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client; and the unavoidable corollary of this standard: If the lawyer has reason to know that a course of conduct unreasonably risks unauthorized disclosure of confidential client information, the lawyer should not engage in such conduct[11] (at least not without the client's informed consent).

This brings us to the NSA surveillance. The extent of the surveillance may never be fully disclosed to the public, but as of now, we have been told in the media that NSA routinely obtains almost all data from within the U.S. that is posted on servers maintained by Microsoft, Yahoo, Google, YouTube, Facebook, Skype, AOL (are they still around?), and Apple, and we must assume other providers as well.[12] Maybe not all of them, but most of those servers are cloud servers. As far as I am concerned, this means that lawyers must assume that any client data that they put on the cloud will be collected by NSA.[13] Indeed, as depressing as this may be, I believe it to be only prudent to assume that any telephone, text, email or other Internet communication is being intercepted and collected (though not necessarily read yet) by some national security intelligence program.[14]

I have seen several recent articles purporting to provide NSA-proof methods of email transmission or Internet posting.[15] But I have no confidence that anything short of going off-line would work.[16] Indeed, there is some indication that taking countermeasures against NSA interception might actually make it more likely that NSA will preserve one's information.[17]

So where does that leave us about deciding whether to put client data in the cloud? There are two separate considerations.

The easiest issue to address is the need to choose an applicable standard for deciding if using the cloud for client data waives virtually all privileges as to such data in light of our knowledge of pervasive national security interceptions.[18] Courts could simply adopt the legal fiction that national security data gathering will not be considered in determining whether exposure of privilege information to outsiders waives the privilege. This makes some sense since that approach (i) might be workable and (ii) the party trying to protect a privilege against waiver is never going to be able to get all intelligence agencies to deny interception

Continued on page 37

and the party trying to prove waiver is never going the get any intelligence agency to admit interception, so we might as well ignore the problem for privilege waiver purposes. Or courts might adopt a privilege for data in the cloud.[19] A third alternative is that we all spend the rest of our careers litigating privilege waivers for data that was put on the cloud. A final alternative is that lawyers abandon the Internet (including VoIP telephony and email) and go back to couriers, carrier pigeons, and (maybe, I am not at all sure about this) faxes and plain old telephone service.

Now back to the second consideration, the ostensible topic of this article: What is our ethical duty for use of the cloud for client data given what we know about national security information? That debate is just starting. I do not pretend to have any definitive answers.

But I do have some suggestions:

First, foremost, and always: communicate with the client (maybe we'd better do that in person and not via the cloud?) about the risks of communicating in the cloud. For local government lawyers I think it is safe to say that there is no major risk involving disclosure due to NSA intelligence gathering — NSA does not generally care about local governments. NSA might collect information placed in the cloud by local governments but will be unlikely to read it. But there are real risks of hacking and other security breaches in the ordinary course of using the cloud and electronic communications generally (and this is a good opportunity to counsel your client about them), and a real risk of privilege waiver from cloud use depending on how the law evolves on this issue.

Second, after fully advising your client, work together to establish parameters for cloud use involving client data. These may range from "go for it" to "never," but probably will settle somewhere between those extremes.

Third, suggest that your client with the lawyer's assistance, explore alternatives to using the cloud for information storage and communications. This includes special precautions for using the cloud, such as special encryption protocols, encoded communications, or limiting use to specified personnel. Your client may decide that the available alternatives are too inconvenient or expensive, or entail equivalent risks without sufficient benefits. Possibly the client will decide to use alternatives only in special, highly sensitive, situations. But we owe it to our clients to suggest that this issue be addressed.

Notes

1. "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." Peter Mell & Timothy Grance, Technical Definition From National Institute of Standards and Technology ("NIST"): NIST Definition of Cloud Computing (Final Oct. 21, 2011) http://csrc.nist.gov/publications/nis tpubs/800-145/SP800-145.pdf (7-page PDF download last accessed Aug. 17, 2012).
2. *See* Cloud Ethics Opinions around the U.S., Legal Technology Resource Center, ABA Law Practice Management Center, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resour ces/charts_fyis/cloud-ethics-chart.html (last accessed Mar. 10, 2013) (table & interactive map with links to opinions).
3. *See* ABA Model Rule of Professional Responsibility, 1.6(c) (as amended 2012).
4. *See, e.g.*, Massachusetts Bar Ass'n Ethics Op. 12-03 (May 17, 2012), http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03 (last accessed Mar. 10, 2013).
5. Whatever "enforceable" means. How would breach of contract damages adequately protect a client from the consequences of leaking highly-sensitive information — particularly since most cloud terms of use include limitations on liability, and even indemnity, provisions?
6. *See*, e.g., New Jersey Advisory Committee on Professional Ethics, Op. 701 [Electronic Storage And Access of Client Files] (undated, but PDF version indicates last modified on May 20, 2011 – refer to publication date in NJLJ for further information), http://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf last accessed Mar. 11, 2013).
7. *See, e.g.,* Alabama State Bar, Office of Gen'l Counsel, Ethics Opinion 2010-02, [Retention, Storage, Ownership, Production and Destruction of Client Files] (undated but PDF version has "last accessed" properties date of Nov. 2, 2010), http://www.alabar.org/ogc/PDF/2010-02.pdf (last visited Mar. 11, 2012).
8. See, e.g., Iowa State Bar Ass'n, Ethics Op. 11-01 [Use of Software as a Service – Cloud Computing] (Sept. 9, 2011), http://iowabar.org/associations/4664/files/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf (last accessed June 28, 2013).
9. Arizona Ethics Op. 09-04, [Confidentiality; Maintaining Client Files; Electronic Storage; Internet] (Dec. 2009), http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704 (last accessed June 28, 2013). In other words, even if you adopt all of the suggestions in this opinion, you might still be acting unethically if the technology changes.
10. Comment 8 (formerly Comment 6) to ABA Model Rule of Professional Responsibility 1.1 (as amended 2012).
11. "Doctor, it hurts when I do that." "So, don't do that!" Steve North: Comedy, Then and Now: Laughing With the Legends of Stand-Up From the 1800's to 2010, http://www.huffingtonpost.com/steve-north/comedy-then-and-now-laugh_b_673361.html (last accessed June 28, 2013).
12. *See* NSA's Prism surveillance program, Times Online, http://www.guardian.co.uk/world/2013/jun/08/nsa-prism-server-collection-facebook-google (last accessed June 28, 2013); Timeline of NSA Domestic Spying | Electronic Frontier Foundation, https://www.eff.org/nsa-spying/timeline (last visited June 29, 2013).
13. *See* Stephen Braun, Anne Flaherty, Jack Gillum, and Matt Apuzo, *PRISM Is Just The Start Of NSA Spying - Business Insider - Associated Press*, http://www.businessinsider.com/prism-is-just-the-start-of-nsa-spying-2013-6#ixzz2WIkgYDqZ (last accessed June 28, 2013); Anne Klinefelter, When to Research is to Reveal: The

Growing Threat to Attorney and Client Confidentiality From Online Tracking, 16 Va. J. of Law & Tech. 1 (2011), http://www.vjolt.net/vol16/issue1/v16i1_1-Klinefelter.pdf (last visited June 28, 2013).
14. As to domestic phone calls, NSA claims it only collects metadata, which in this context apparently means call log data rather than the substance of communications. *See* Rutrell Yasin, NSA's intell gathering puts the spotlight on metadata ~ GCN, http://gcn.com/articles/2013/06/26/nsa-intell-gathering-spotlight-metadata.aspx?s=gcntech_270613&m=1 (last accessed June 28, 2013).
15. *See*, *e.g.*, Peter Bright and Dan Goodin, Encrypted e-mail: How much annoyance will you tolerate to keep the NSA away? | Ars Technica, http://arstechnica.com/security/2013/06/encrypted-e-mail-how-much-annoyance-will-you-tolerate-to-keep-the-nsa-away/?utm_source=Ars+Technica+Newsletter&utm_campaign=970d84696c-September_02_2011_Newsletter&utm_medium=email&utm_term=0_0adf3ee3d9-970d84696c-61721097 (last accessed June 21, 2013); Joan Walsh, Encrypt your emails, evade the NSA - Salon.com, http://www.salon.com/2013/06/11/evade_the_nsa_with_these_safe_surfing_tips_partner/ (last visited June 28, 2013);
16. *See* The Motherboard Guide to Avoiding the NSA | Motherboard, http://motherboard.vice.com/blog/the-motherboard-guide-to-avoiding-the-nsa (last accessed June 28, 2013).
17. *See* Dan Goodin, Use of Tor and e-mail crypto could increase chances that NSA keeps your data | Ars Technica, http://arstechnica.com/tech-policy/2013/06/use-of-tor-and-e-mail-crypto-could-increase-chances-that-nsa-keeps-your-data/ (last accessed June 29, 2013).
18. The known "presence" of strangers traditionally waives the privilege. *See* Rhone-Poulenc Rorer Inc. v. Home Indem. Co., 32 F.3d 851, 862 (3d Cir. 1994). This raises issues beyond the scope of this article, but the argument for waiver is that the known practice by NSA to collect data from cloud servers would waive the privilege even if no attorney-client communications were intercepted either because the client took insufficient precautions to protect confidentiality or because the carelessness evidenced lack of intent to keep the communication privileged. *See* T. Noble Foster & Christopher R. Greene, Legal Issues of Online Social Networks and the Workplace, 18 J.L. Bus. & Eth. 131, 135 (2012) (posting on Internet waives privilege because no objective expectation of privacy, even using password protection).
19. *See* Jacob M. Small, Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet, 23 Geo. Mason U. Civ. Rts. L.J. 255 (2013). I do not think this would ever happen, which of course means that the chances are quite good! ML

Supreme Court *Cont'd from page 29*

approval—a remedial proceeding— or if *Younger* abstention only applies where the state brings a party before the court or administrative board in a coercive proceeding. Most remedial proceedings happen on the local level and involve zoning variances, the denial of gun permits, and the like. The question is whether a federal court should be able to review this type of decision immediately or whether it should abstain until the state proceedings have ended. The SLLC will file an *amicus* brief in this case.

Next term is already shaping up to be an exciting one for local governments, and the Court is likely to grant thirty or so more petitions before February. Although the cases set for argument so far might lack the glamour and media hype of this summer's rulings on same-sex marriage, voting rights, and affirmative action, the issues before the Court deal with some of the essential mechanisms of local governance across the country. Whether the Justices will rule in favor of local governments remains to be seen.

(Victor Kessler was a summer intern at the State and Local Legal Center (SLLC), headquartered in Washington D.C. IMLA is an associate member of the SLLC, which files Supreme Court amicus briefs on behalf of the Big Seven national organizations representing state and local governments. IMLA appreciates the contribution by SLLC and Mr. Kessler to Municipal Lawyer.) ML