CLOUD COMPUTING: PRIVACY STORM ON THE HORIZON?

Andrew C. DeVore

Good morning, I'm Andrew DeVore. It is a pleasure to be here. This has been—for someone who's sort of a geek in this stuff—an enormously interesting morning so far.

I'm a former Federal Prosecutor in the Southern District of New York where I started the Computer Hacking and Intellectual Property Unit, one of five such units started across the country by the Department of Justice. In that capacity I got to spend a lot of time investigating and digging around in the wreckage of information privacy and security incidents and prosecuting crimes involved with computers and the Internet. In my law firm I spend a lot of time on the other side of that kind of analysis—that is, advising a broad range of companies on an equally broad range of issues to try to help them avoid being in the kinds of privacy and security incidents that subject them to notification laws, criminal sanctions, regulatory investigation, and the prospect of litigation.

There's a lot going on here and I think this has been a great introduction to what some of the core issues are that are driving that analysis in the corporate world. I want to try to focus on a particular instance of something that's happening now and take a look at some of the privacy and security issues raised by that undertaking. What I'm talking about is cloud computing. I'll talk a little bit about what cloud computing means, but also suggest that, in light of all of the privacy and security considerations that have been the subject of people's remarks this morning, I think there's a real issue that is still latent with regard to cloud computing that really needs to be identified and examined as companies and individuals push out and use cloud computing services.

I have a couple of quick disclaimers. I'm here on my own, not on behalf of my firm or any of my clients. I also have about ninety minutes worth of material to do in twenty-five minutes so

I'm going to go very lightly on some of these things and I'm going to focus more intensely on some pieces. Also if anybody wants a copy of the slides, I'd be happy to make them available, just give me a card or your e-mail address at the close.

So the big picture of the issues I will focus on today: First, what are we talking about? What is cloud computing? Next, I will offer some quick insights regarding why all the fuss about cloud computing? Next, I'll discuss some of the security implications involved in the use of cloud computing services, as well as privacy implications. Then I'll conclude with some practice and tips and guidance.

What is cloud computing? I'm going to read this brief definition and then we'll try to make sense of what it is. The National Institute of Standards and Technology, NIST, says cloud computing is: "A model for enabling convenient on-demand network access to a shared pool of configurable resources, for example, network servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction." What does this really mean? It means services provided by a third party, hosted by a third party. It may be applications. It may be storage capacity. It may be some combination of the two. It may be a network of collaboration services that are accessible and are able to be used via the Internet from pretty much anywhere.

There are a number of different models. What is available? One of the biggest categories is on-line applications. This means the ability to access and use online the kinds of tools that we all use now in our work, in our business, to do the things that we do: documents, Excel spreadsheets, sales force management, and all sorts of business productivity applications, as well as simply storage capacity. All of this information that we've been talking about all morning is being constantly acquired and used by companies, and I think we all recognize the extraordinary value of that information. The corresponding need for storage capacity and the ability to handle and process that information have grown extraordinarily and will only continue to grow. And that's part of the reason why cloud computing is becoming such a big deal.

So why is cloud computing such a big deal? There is little question that it offers tremendous potential advantages, particularly in efficiency and cost savings. Companies can gain substantial advantages by not having to acquire your own

services, your own infrastructure, your own professionals to maintain the applications to make sure you have what you need, make sure that there are appropriate security protocols in place, make sure that there are appropriate privacy rules, policies, and procedures governing the information that you as a company have and use. All of those things can be provided by third-parties in the cloud. And the ability to access these kinds of applications and services remotely via simple Internet connection, and not have to maintain those things yourself, offers real practical advantages.

Cloud computing also offers potentially significant advantages with regard to cost savings and efficiency. Companies are often obligated to acquire much more computing capacity than they need, and to apply the corresponding security, technical, and support requirements to all that capacity. But much of that capacity is underutilized—that's just the way computing works. In contrast, by being able to use a third-party to run your services, you don't have to support anything more than what you need. These third-party services tend to be pay-as-you-go, and that offers enormous advantages for companies that are involved in processing and using all of this information. Computing in the cloud also offers potentially extraordinary collaborative opportunities. And companies are very interested in having services that make it easy for workers across the organization and across the world to use those services collaboratively.

So is this really a big deal? Yes it is. Gartner projects that revenue for cloud service providers this year alone will be fifty-six *billion* dollars. That number is supposed to go up 20% year over year, so by 2013 revenue is projected to surpass one hundred and fifty *billion* dollars. So this really is a big deal. And as a result companies, governments, and others are all pushing out aggressively to use these services. They really do offer potentially substantial cost savings and other advantages.

A couple of quick examples. First, President Obama's CIO, Vivek Kundra, recently announced a big government cloud computing initiative. He announced in particular the www.apps.gov site, a site where all government entities are going to be able to go to provision applications and services previously approved for use in government service. That alone is a really nice nutshell example of the potential efficiencies and savings that cloud computing offers. Kundra tellingly also described this move as the beginning of a "journey for the Federal Government

over the course of the next ten years to push out dramatically into the use of cloud computing services."

Interestingly—a little side note here that I will return to when I discuss practice tips—Kundra has also made clear that the Government will *not* be putting classified and sensitive data in the cloud; they're going to maintain their own services and infrastructure for truly sensitive information.

Second, Los Angeles just announced that they're going to engage Google to provide their e-mail and office services through Google Docs, a $7.25 million dollar contract. The Los Angeles Times accurately described the competition between Google and Microsoft for that contract as "a rivalry that could help determine the future of both companies." Again, this is a big deal. These major providers recognize that this may well be the future of computing, particularly in the corporate world.

Cloud computing also offers the potential for great security advantages. Most small and medium-sized companies just don't have the resources to provide the security that they should have in place to protect their electronically stored information. This is something that I and my colleagues see all the time as we go into companies and try to help them understand what their privacy and security obligations are and try to meet those obligations. It's very difficult. It's very challenging. There are a lot of moving targets with regard to what the rules are, but the reality is there is a lot that needs to be done and a lot of companies, particularly smaller companies, just don't have the resources to get it done in the right way.

Here again, if you move that information to a third-party provider that provides expert services, typically on a vast scale, you're going to get built in the very best security protocols and the very best information management practices, and as a result you're going to get a substantial benefit in terms of addressing certain of the major risks that you face on privacy and security.

Engaging cloud services may also help to eliminate the risks posed by insiders, as insiders so often are associated with breaches. For example, one 2008 study found that almost 88% of all breaches involved insider negligence. I also have to say that, both as a prosecutor and now in private practice, I see all the time that breaches of information privacy and security involve insiders who simply take stuff when they walk out the door. Or others, whose access is not eliminated when they walk out the door, who come back in, destroy things, or take things and start

the competing business. Unfortunately, it is part and parcel of how this world works, and by using a third party provider you can substantially reduce those risks. And that can be very attractive—particularly as you really dig in and start to understand what those risks are.

So with all these potential upsides, what are the potential privacy and security risks associated with cloud computing that I mentioned at the outset? Well, from my vantage point, cloud computing raises some significant potential down sides. You have the benefit of this professionalized, high quality security and infrastructure management, but you also are at the mercy of the third party if they make a mistake. You also have very high value collections of data because in using cloud services you tend to put all your data in one place. At the same time hackers, as a previous speaker mentioned, are becoming increasingly sophisticated. They're organized, professional groups and they're going after this data in very methodical and sophisticated ways. They see these high value targets and they are going after them big time and trying to gain access to that information. It's also difficult to encrypt data in the cloud. That's something that probably will be addressed in time, but it remains an issue today.

So as a result what do we get? We get real problems that have already surfaced in connection the use of cloud computing services that are already commonplace. For example, in October of this year, as many of you may have heard, all of the data users stored and exchanged using their T-Mobile "Sidekick" handheld devices was destroyed by a Microsoft Subsidiary—Danger, Inc. After a server meltdown—stuff that we've all experienced with our own home computers—T-Mobile notified users that they did not have backups of the user information stored on that server and the information was gone. So anybody who had their information in the cloud with that service provider lost the information.

Another example is Google Docs, the cloud solution at the heart of the L.A. contract I just mentioned. I can't tell you how many businesses use Google Docs for their business productivity applications. It's all online, it's easy, it's seamless, you can make it look like your own. With a glitch on permissions, however, Google Docs recently allowed non-authorized users to view the private content of others. Now take that example and put yourself in the context of the City of Los Angeles using Google Docs—what a huge problem, with huge potential implications on

privacy and security and all the ramifications of exposing very sensitive data.

Then there is the recent example of Twitter. Interesting in part because once somebody successfully got into the system, they changed user passwords and sent out tweets posing as a number of high profile individuals, including an unnamed newscaster where the tweet was, "I'm high on crack right now, can't come into work today." It may seem funny, but it really is again a very telling example about some of the risks here. Imagine something like that in the corporate context. Imagine something like that going out on behalf of your company unauthorized.

So now, to get to what I believe is the very heart of the matter in my remaining six minutes or less: there are very serious privacy implications with regard to the use of cloud computing that I think are still largely unexamined. They start with the Electronic Communications Privacy Act and the law underlying the act, a number of the other laws that have been mentioned here today, and terms of service. As I mentioned when I began, these are things that I believe have not yet hit the radar screen with regard to the use of these services, which is expanding dramatically. In fact, I think it will take the ChoicePoint breach of this realm or the Sears breach of this realm to really put this stuff on people's radar screen. But I can pretty much guarantee you that that will happen.

The heart of the privacy issue with regard to cloud computing is the fact that you are handing over potentially highly sensitive and private information to a third party to store and process. What the law says, and it's quite clear, is that if you have private confidential information, you have certain privacy interests and corresponding legal protections for that information so long as you maintain the privacy and secrecy of that information. If you give that same information to a third party, however, you effectively lose those protections. That's the way the law works.

United States v. Miller is in one of the seminal cases here. In *Miller* the Supreme Court said, "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to the government authorities even if the information is revealed on the assumption that it will be used only for a limited purpose." In that case there were bank records voluntarily conveyed to a bank. Bank employees could look at those records in the course of their employment and the Supreme

Court said there's no Fourth Amendment protection, there's nothing that is going to support what the defendant in that case claimed was a privacy interest in those records.

In response, Congress passed the Electronic Communications and Privacy Act (ECPA) in 1986. It's a very complicated statute—it could be the subject of a separate talk and is as part of the Internet and Computer Crimes class I teach at Columbia Law School—but in summary ECPA put in statutory controls intended to approximate Fourth Amendment and other protections for electronic communications and other information stored electronically. But think about it. That law was passed in 1986. It's been amended and tweaked a little bit since, but what we're talking about is applying this 1986 law to what's going on almost 30 years later in a world that is changing dramatically every couple of years if not every couple of months, with the law struggling to catch up at every step.

And this raises a number of core questions, the most fundamental of which is whether the varying levels of protection that the Act sets forth make sense in this world? I won't spend too much time going through the details of the Act, but in short it provides graduated protection for electronically-stored information. The most sensitive information under the Act—and so the information with the greatest protection—is the contents of e-mail communications that are in transit from the sender to the recipient. So long as those communications are in transit they're considered to be subject to the highest protection. So you have to have a search warrant to get the content of electronic communications that are in transit from one sender to another.

But as you go down from there, the protection goes down correspondingly. And so less process is required to get the information that is considered under the Act to be less sensitive. And what is not an electronic communication in transit from one user to another? The great majority of company business records. They don't really have anything to do with that. Thus, in three minutes or less, it appears that ECPA really doesn't provide protection for that kind of corporate information. The highest level of protection is reserved for e-mail communications in transit. But, in the context of a civil proceeding, the Act affords virtually no statutory protection—and there is correspondingly little Constitutional protection—for the great bulk of business communications or other work documents stored with a third party online.

Think about the implications of that as companies, particularly large companies and Governments, push out into the use of cloud computing for the full range of their business applications and support services. All of this potentially highly sensitive and confidential business information is going to be stored and processed in the cloud, in the hands of third parties not subject to either Constitutional or statutory privacy protections that otherwise may be available in connection with that information.

In addition, there are a whole other host of laws and considerations at play that are also largely unexamined. For trade secrets, in order to maintain a trade secret you have to take steps that are reasonable under the circumstances to protect the secrecy of the information. Is putting your sensitive information in the hands of a third party provider not subject to privacy protections and controls reasonable under the circumstances? Nobody's looked at that question, but I think it's a real question.

Contractual data obligations. Companies may be obliged by virtue of their arrangements with third parties to maintain the secrecy and confidentiality of certain information, but cloud solutions may be unable to satisfy those obligations.

And the same kinds of questions arise in connection with bankruptcy. This is a market where companies pop up and disappear all the time. The best get big and get acquired; the worst disappear completely or go into bankruptcy. What happens when the companies disappear? What happens to your information stored on their servers? What is the backup situation? Can that information be disposed of as an asset of the company in a bankruptcy? This hypothetical raises the same kinds of questions and, again, those questions remain largely unexamined.

Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), which have been well covered so far today, all potentially raise the same kinds of questions.

"Terms of Service" is another critical area where companies and individuals have to look as they think about employing these cloud services. Most Terms of Service allow the provider of the cloud service access to data, the ability to view data, and the ability to turn data over in the event that the Government or a third party asks for it. Often that's true without any notice to the consumer. If you have contractual controls in place that require that you maintain the confidentiality of your information,

or you have particular concerns about the privacy and secrecy of that information, you better look at those terms of service as you make a judgment about whether any cloud provider can satisfy those requirements.

In my few minutes remaining, I will just touch on a handful of practice tips and guidance. For all organizations that are thinking about using cloud service providers, in my estimation, you have to think about these issues. You have to take stock of the information that you have and use. You have to assess the sensitivity of that information. You have determine about the controls that may well already be in place or that are required to be in place with regard to protecting that information, contractual and otherwise. And you have to look at the Terms of Service for the cloud provider and see if they could possibly satisfy the requirements you have for the information you intend to process, use, and store using cloud services.

For larger organizations which may have substantial bargaining power, including again, for example, the City of Los Angeles, you have to build into the contractual arrangement with the cloud provider the controls you need to make sure you get the protection you want. You need to do all you can to ensure that the provider has security protocols in place to protect the security of your information, privacy controls, and in the case of Los Angeles, potentially severe financial or other penalties in the event of a breach. You need to build in incentives to make sure that your privacy and security obligations can be satisfied.

Companies may also be well advised to consider a hybrid approach, such as that Vivek Kundra has suggested. The Government is going to push out into cloud computing, particularly in the apps.gov context. Making applications available across the Government makes a lot of sense. But for truly sensitive and confidential information, think seriously before putting that information in the cloud at all in light of all the privacy and security issues that are arising. Kundra says the government won't be putting that kind of information in the cloud.

And, finally, think about encryption, which has become something of a baseline norm and best practice for the protection of sensitive information, and which may help to satisfy some of the concerns that I've identified.

Thank you.