CLOUD COMPUTING

Olshan, a New York law firm that represents clients on advertising, marketing, and promotions, scheduled a seminar on Cloud Computing: Keeping Employee, Customer and Confidential Information Safe in October 2012. Cloud computing offers numerous advantages such as more storage space and less maintenance of applications, but there are concerns on data security and privacy. Businesses in advertising and marketing may collect a lot of customer data and not know if transferring information online or keeping data in the cloud is safe. Cloud computing offers scalability. For example, ad serving can be increased or reduced. It is possible to store various ads and make them available on demand, without investing in infrastructure. Cloud computing facilitates collaborative activities for advertisers and marketers. This allows people to be more creative, and gain access to more resources. When information is sensitive, the cloud may not be safe for transferring data to a third party when anyone who has access to an account password can sign on to an account no matter where the person is. Advertisers and marketers using cloud applications need to deal with negotiating contractual protections, and inspect privacy- and security-related due diligence. When using cloud technology, people in marketing or advertising need to be aware of the difference between privacy and confidentiality, data privacy and security issues, safeguards for transferring data to the cloud, and allocation of compliance responsibilities between clients and business providers. The First Amendment to the U.S. Constitution and common law protects privacy, but not confidentiality. When people want confidential data protected, they satisfy the burden of proving a compelling government interest requires secrecy, and sealing of records must be narrowly tailored to serve that overriding government interest. The U.S. Supreme Court has stated in United States v. Miller, 425 U.S. 435 (1976): "The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Protective orders, which govern the exchange of information outside of a public docket, between private litigants, are obtained pursuant to a "good cause" standard. When such information is filed with a court, it becomes a public document subject to the right of public access. For such information to remain confidential, a party must rebut the presumption of access with "compelling reasons." Pintos v. Pac. Creditors Ass'n, 504 F.3d 792, 801 (9th Cir. 2007). This showing must be "supported by specific factual findings that outweigh the general history of access and the public policies favoring disclosure, such as the public interest in understanding the judicial process." Dagdagan v. City of Vallejo, 2011 U.S. Dist. LEXIS 116393 (9th Cir. 2011) citing Kamakana v. City and County of Honolulu, 447 F.3d 1172, 1178-79 (9th Cir. 2006).