NNEDV

Cloud Computing

How the Technology Works:

The term "cloud" basically refers to the Internet. Cloud computing offers simple ways to have online access to your agency's computing needs. Specifically, cloud computing companies offer the option to place portions of your agency's computing and data onto Internet-accessed servers that somebody else (e.g. the third party cloud computing provider) owns and manages; this is rather than storing your data and applications on computers, dedicated servers, and back up drives that your agency owns and maintains.

Common services that cloud computing providers might offer include online remote:

- Email access and storage;
- Multi-person editing and sharing of documents or presentations;
- Data and database management with access from multiple office locations;
- Photo and video sharing and storage;
- Full or partial system and data backups; and,
- Server and application management including anti-virus, anti-spyware, and operating system updates.

Cloud computing providers can be small regional companies with servers located within the same jurisdiction as your office and constituency, or, large global corporations (e.g. Google, Microsoft, Amazon, Yahoo) that own hundreds of Internet-connected cloud computing server warehouses scattered across various jurisdictions globally. Because the computing is done "in the cloud", the offsite location where data is processed and stored may move around depending on how the provider operates its cloud computing services. Cloud computing services can be impacted by many things including Internet outages, connectivity speeds, unauthorized access and server crashes.

How are Agencies and Partnerships Using It?

- Some cities are moving services and data into the cloud with a goal of saving money. This sometimes results in a city's law enforcement or court computing systems being automatically moved into a cloud service before they can assess the potential impact on victim confidentiality, privacy, and safety.
- Some agencies and coordinated community partnerships are using cloud computing services selectively to facilitate non-confidential online work tasks. For example, a partnership with agencies that are not co-located might use a cloud computing service to enable staff from several office locations to get online together and efficiently edit non-confidential documents or presentations.
- Other agencies and partnerships are using cloud computing providers as online spaces to house select prevention, public education and awareness outreach campaigns. For example, some agencies have used online photo sharing services to display an online campaign where they invite community members to upload photos of themselves holding signs with violence prevention messages.
- Agencies and partnerships in regions that have dealt with weather-related disasters have been exploring cloud computing services as part of emergency preparedness strategies.
- Some agencies and partnerships use cloud computing services to store and backup agency documents, applications and data that does not include personally identifiable or confidential information.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

Cloud Computing

Benefits and Risks

Cloud computing can seem appealing because it enables agencies to offload computer and data management tasks to the third party cloud computing provider. That third party provides a simple online point of access and takes responsibility for storing, protecting and backing up your digital files and applications at the offsite location. This can relieve agencies of the ongoing obligations to troubleshoot and address computer and application crashes and security issues. It can also offer increased flexibility for staff who want to access data or services from various office or offsite locations. However, cloud computing can leave agencies vulnerable to risks including confidentiality and privacy breaches, and, unreliable access to agency data and systems.

Technology and security:

- Sometimes moving to cloud computing services can decrease the number of higher-end computer servers your agency needs, resulting in less office space needed to house the servers, fewer onsite computer personnel, and less staff time spent maintaining and upgrading onsite software and hardware systems. While this can decrease onsite costs, there are often offsite costs associated with a cloud computing provider operating and maintaining your computing systems.
- When information and applications are stored remotely, they can be accessed from any permitted device with an Internet connection, including laptops, tablets, and smart phones. Thus, agencies still need to address security and privacy issues for each device accessing the agency's cloud computing spaces and services. Security issues and privacy risks can also increase in complexity when data or data access is distributed across many devices and a range of locations.
- With online access to remote files, there are security risks and vulnerabilities of unauthorized access by other customers, the provider's employees, or hackers.
- How reliably you can access your agency's data and services is impacted by slow connectivity speeds, Internet outages, service provider crashes and data loss, the quality of the provider's technical support, their policies regarding data backup and storage, and, the ease of transferring your data and services from one cloud provider to another.

Legal issues: Confidentiality, privacy and informed consent must be addressed each time an agency or partnership considers using a cloud computing service.

- A cloud computing provider is a third party which raises different sorts of legal risks regarding outside access. Agencies and individuals should take precautions to ensure that they are fully complying with federal confidentiality laws and other professional obligations and protections provided under attorney-client, doctor-patient, victim-advocate and other "privilege" or confidentiality laws. For example, lawyers have distinct legal obligations regarding outsourcing, client confidentiality and their duty to remain aware of the evolving risks and benefits of using a technology. Thus, lawyers should conduct due diligence on the benefits and risks of outsourcing to the cloud and fully address issues including confidentiality, security, control and client consent.[1]

[1] The American Bar Association (ABA) and its' Commission on Ethics 20/20 (http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html) provides evolving guidance and recommendations to their members.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.

NNEDV

Cloud Computing

- Agencies should analyze the cloud computing provider's policies and ensure that your planned uses keep you in compliance with all relevant state, territorial, tribal and federal laws and regulations. For example, assess your use to ensure you comply with the U.S. Privacy Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Violence Against Women Act (VAWA) or any additional laws or professional codes of contact that may apply to the confidentiality, privacy, maintenance, storage, and disposal of your agency's records?

Public awareness activities: It is best practice to provide transparent statements about the benefits, risks, and privacy options of any cloud computing service that your agency decides to use in a public awareness campaign or outreach activity. Anyone being encouraged to participate in your campaign should be informed upfront about the privacy options, benefits, and risks of the particular cloud computing service so they can assess their own safety and privacy tradeoffs before participating. See also, "Privacy Considerations When Posting Content Online" and "Online Privacy and Safety Tips".

Things to Consider:

- Who owns your agency's data once it is in that cloud – is it you or the cloud computing provider?
- What do the provider's policies and terms of service say? Does the cloud computing provider reserve the right to use, disclose, access, or make public some or all of your agency's data? How does this impact your confidentiality and victim safety obligations?
- Can the provider deny an agency access to their own data?
- What data protection, privacy and records confidentiality laws apply to your data? Is the data stored on servers within your state/territory, elsewhere in the U.S. or internationally? Which jurisdiction's rules apply in case of conflict?
- What are the provider's policies for responding to (or when appropriate, resisting) law enforcement or other legal requests for access to information, and, for notifying customers of security breaches? Do they have an enforceable obligation to preserve your agency's confidentiality?
- What security measures are in place to protect your agency's data and services? Is all data encrypted and who has the encryption key?
- If the agency decides to switch cloud computing providers, is there a method in place to easily move your applications and data between providers?
- If the provider goes out of business, what happens to your agency's data and services?

For more information about your individual state's victim advocate confidentiality provisions, see our Summary of U.S. State Laws Related to Advocate Confidentiality. For more information about VAWA provisions regarding consent for releases of information, see NNEDV and the Confidentiality Institute's pieces on, Survivor Confidentiality and Privacy: Releases & Waivers At-A-Glance and FAQ's on Survivor Confidentiality Releases.

Supported by US DOJ-OVW Grant #2007-TA-AX-K012.Opinions and recommendations expressed are the authors' and do not necessarily reflect the views of DOJ.