

CONSUMER PRIVACY & IDENTITY QUARTERLY

THE CLOUD IS A BREEZE:
SIMPLE STEPS TO
SAFEGUARD YOUR DATA
AND PRIVACY ONLINE

5

WHAT DID I JUST ACCEPT?
THE PRIVACY POLICIES
THAT GOVERN THE CLOUD

8



VOL N°3 ISSUE N°1

10

BRING YOUR OWN
UMBRELLA: MANAGING
CLOUD SECURITY RISKS

CLOUD
COMPUTING



DISCLAIMER

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

IN THIS ISSUE:

USING THE CLOUD, PREPARING FOR THE STORM

Email. Social networking services. Smartphones. Online gaming. Google Docs. They are all a part of the growing system of cloud-connected hardware, software & services that 3.8 billion consumers are using to transform the ways they live and work. - *Page 4*



THE CLOUD IS A BREEZE: SIMPLE STEPS TO SAFEGUARD YOUR DATA AND PRIVACY ONLINE

When you save selfies to Dropbox or upload your address book to LinkedIn, where does that data go? - *Page 5*

ALSO INSIDE:



WHAT DID I JUST ACCEPT? THE PRIVACY POLICIES THAT GOVERN THE CLOUD - *Page 8*



LOCK BEFORE YOU UPLOAD: HOW TO ENCRYPT DATA FOR THE CLOUD - *Page 11*



FUTURES: COMPANIES CAN FACE MAJOR FINES FOR LOSING YOUR DATA UNDER NEW EU REGULATION - *Page 12*



USING THE CLOUD, PREPARING FOR THE STORM

"Life in the cloud requires vigilance and safeguards."

Your new Amazon Echo Spot wakes you up every morning. News streams from your smart TV while you check email and browse social media updates on your iPhone. A calendar app flashes your next appointment but Google Maps alerts you that local trains and buses are running behind schedule. Better call an Uber and send a quick Hangouts message to your team telling them you might be late.

Your day—courtesy of: The Cloud.

Email. Social networking services (SNS). Smartphones. Online gaming. Google Docs. They are all a part of the growing ecosystem of cloud-connected hardware, software, and services that 3.8 billion consumers worldwide are using to transform the ways they live and work.

The cloud is a network of Internet-connected servers that store data in a central location, allowing individuals to access and share information from multiple devices, and run specialized applications. Instead of accessing data on your computer's hard drive, data and software is accessed over the Internet. Millions of individuals depend on cloud services to backup devices, store files, conduct transactions with businesses, and access critical financial and health records. It is almost impossible to send an email, surf the web, or turn on a smartphone without personal data being collected, transmitted, stored, and analyzed on hundreds of servers around the world.

Despite one-third of computer users wrongly believing they do not use the cloud, according to a 2017 survey from research firm Clutch, the technology is ubiquitous. Internet users will store 915 exabytes of files in data centers globally by 2020, five times more than in 2015, according to Cisco Global Cloud Index: Forecast and Methodology, 2015-2020.

But with greater access comes increased risk. Privacy advocates and security experts warn that some cloud services employ weak security safeguards—storing data unencrypted or in overseas countries with fewer privacy protections—that could compromise your privacy and, as the number of data breaches rise, leave data vulnerable to theft.

There were 1,339 reported data breaches in 2017, according to the Identity Theft Resource Center, up from 780 breaches in 2015. Government agencies, including the federal Office of Personnel Management, and large private entities, including Equifax, have been shown to be vulnerable to data theft.

Meanwhile, the data security and privacy policies of many commercial cloud services are lacking. About 67 percent of cloud services do not specify that users retain ownership of uploaded data, according to Netskope's 2017 Cloud Report, and 80 percent of companies do not encrypt data stored on their servers, making it more vulnerable to theft.

Of course, all of this is confusing to users, many of whom do not understand the cloud or how to protect their data. In this issue, you will read about how to safeguard your privacy and data in the cloud. The feature article, "The Cloud is a Breeze," will walk you through simple steps to secure the most popular services, while "I, Cloud" provides tips for custom alternatives for better cloud security.

NEXT: The Cloud is a Breeze

CONSUMER PRIVACY
& IDENTITY QUARTERLY



THE CLOUD IS A BREEZE: SIMPLE STEPS TO SAFEGUARD YOUR DATA & PRIVACY ONLINE

When you save selfies to Dropbox or upload your address book to LinkedIn, where does that data go?

The Cloud? Yes. But can you explain what the cloud is, how it works, or how information stored there is protected?

Few consumers can, though every year millions more entrust photos, contacts, medical records, and other sensitive files to a growing number of cloud service providers (CSP). The connection between personal devices and the cloud is so seamless—(e.g. automated photo backups and appointments automatically added to your calendar from an email)—that an estimated one-third of users do not know they use cloud applications.

As a result, many users are not taking steps to safeguard their data. That makes the oceans of personally identifiable information (PII) in the cloud a rich target for hackers, including the group that breached Equifax last year and exposed the financial data of 143 million consumers.

This article will walk you through the security risks of some popular cloud applications and provide suggestions to protect your privacy.

Understanding the cloud

The cloud is a collection of networked computers that store and manipulate data. The software running the servers exists only, or mostly, on the Internet and is accessible through apps and web browsers. Your data

is stored on remote servers instead of the hard drive of your smartphone or PC.

Many devices have limited storage, making the cloud a convenient way to backup and access files. The cloud also makes computing more convenient. Emails are stored on smartphones and saved on servers so they can be accessed from multiple devices. Social networking services (SNS), such as Instagram and Twitter, grant millions of users access to shared resources. However, consumers are not always aware when they are using the cloud.

In a 2017 survey, Clutch, a research firm, found that one-third of respondents said they do not use the cloud despite previously admitting to using at least one cloud-based application. Another 13 percent of respondents answered “unsure,” meaning nearly half of surveyed individuals do not realize that private data they are sharing with apps is leaving their devices and being stored on servers around the world.



Many CSPs offer two-factor authentication, requiring a one-time code in addition to a password, for added security.

*Peruse CSP options and enable this feature, if available.

When users store or share data in the cloud they are at the mercy of corporate privacy policies. Follow these suggestions to better secure your data and privacy.

Cloud storage

Risks: CSPs, including Google and Amazon, can look at data stored on their servers, using automated systems to scan it for advertising purposes and malware detection. Most CSPs do not encrypt stored data. The companies that use encryption typically store encryption keys on their servers thus leaving data vulnerable to theft.

Continues on Page 6...

Solutions:

- Review privacy policies to determine how data is stored and used. Ensure services meet federal and state privacy requirements.
- Encrypt data before uploading it using services, such as Boxcryptor, or use CSPs, such as SpiderOak, that offer end-to-end encryption and store encryption keys on devices, not their servers.
- Disable automatic uploads. Only upload files to the cloud when necessary.
- Monitor sharing settings. Do not share files or make them public unless necessary.
- Do not use a single CSP. Separate files and back them them with multiple CSPs to reduce risk if one CSP is breached.

Email and messaging

Risks: You might not think of Gmail and Whatsapp as cloud applications, but they are. They store the content of your conversations, shared images and files, lists of contacts, and the identities of individuals with whom you interact.

Solutions:

- Use secure chat apps, such as Signal, that encrypt data end-to-end and only store encryption keys on user devices.
- Purge chat histories regularly and use self-destructing messages.
- Do not discuss sensitive topics or share sensitive data in unsecure applications.
- See the IAPM Guide's Smart Card on Secure Chat Apps for more guidance.

Password Managers

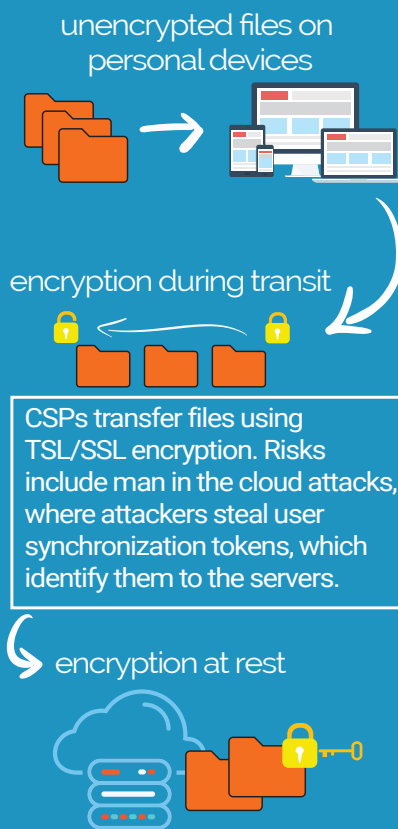
Risks: Storing passwords in a cloud service, such as Lastpass, is convenient but not always secure. A bug in the Lastpass browser extension, identified in March 2017, could have allowed hackers to steal user data.

ENCRYPTION IN THE CLOUD

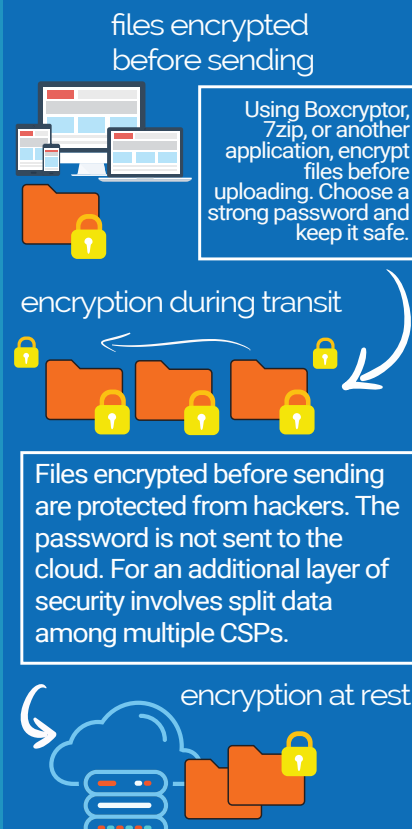
Encryption protects digital data—messages, images, and other filetypes—by transforming it into indecipherable code that can only be unlocked with a password or encryption key. Cloud storage providers (CSP) do not always encrypt user data and the rising number of data breaches leaves consumers vulnerable. Here are some tips to boost your security in the cloud.

Common Encryption Algorithms	TLS/SSL	Protocol used for secure exchange of data between devices, web browsers and servers
	AES	Encryption standard developed by US government to safeguard classified information
	3DES	Protocol developed to strengthen DES encryption; data is encrypted using three keys
	Blowfish	Open source protocol developed to replace DES. No known successful attacks

Standard Cloud Encryption



Enhanced Cloud Encryption



Concludes on Page 7...

Solutions:

- Avoid cloud-based password managers. Use services, such as KeePass, that store passwords locally.
- Understand security and privacy policies. Read user reviews and pay attention to any security issues raised.
- Change all passwords every couple of months.

Finance

Risks: Finance apps, including Mint and Apple Pay, allow users to aggregate and manage credit reports, bank and investment accounts, and payment information. Finance CSPs have suffered relatively few breaches, but there are ways to maximize security.

Solutions:

- Use longer passwords.
- Do not use finance apps on public WiFi networks or use a trustworthy virtual private network (VPN) to secure the connection.
- Utilize fingerprints to access apps.



Location

Risks: Many apps request location data for targeted ads or to provide services, such as weather. When location data—obtained from GPS, WiFi networks, and nearby cellphone towers—is paired with PII, it can be used to identify individuals and create and store detailed maps of an individual's travels.

Solutions:

- Restrict access to GPS and network location data on devices.
- Turn off GPS, WiFi, and Bluetooth, and disable location services when not in use.
- Delete location data, if possible.
- Avoid using services that store location data.

Social networks

Risks: SNS users upload large volumes of PII, including photos, videos, relationships, addresses, email addresses, and interests. The data can be used for targeted advertising and shared with third parties.

Solutions:

- Keep SNS private. Only connect or share information with trusted contacts.
- Limit PII you share and remove sensitive information from photos and other items.
- Be cautious when granting third-party applications access to data.

Trust, but verify

It is not always easy to determine how CSPs use your data, how many copies exist and where they are stored, or whether data is expunged when you choose to delete it. Reviewing privacy policies, adding your own layers of encryption, and exercising caution before clicking “upload” may make the cloud less convenient, but your data and privacy will be much more secure.



WHAT DID I JUST ACCEPT? THE PRIVACY POLICIES THAT GOVERN THE CLOUD

When signing up with cloud service providers (CSP)—which can compile disparate bits of information users share from around the Internet to become privacy-killing behemoths—those often ignored privacy policies and terms of service (TOS) are required reading.

Whether performing PC backups or storing photos, using a CSP is like loading your private information onto a stranger's computer—and trusting them to keep it safe, not peek at any of it, and not misuse it. You would never do that, of course, and if you did, you would quiz them for hours until you were comfortable. Using a CSP is no different.

Google, Facebook, Apple, and Amazon are top CSPs for most consumers so those are good places to start reading.

Google: Users grant the company a worldwide license for uploaded content, an agreement that covers Google Drive, YouTube, and Gmail. But each application has specific terms.

- In Google Drive, Google's license to scan and otherwise manipulate files to operate its services remains in force until files are deleted (which involves deleting files from the main directory and again from the trash folder), regardless of whether an account is active.
- YouTube can delete files at any time, terms can change without notice, and the service can keep copies of deleted videos.
- Google's automated systems scan emails and files uploaded to Drive for targeted advertising and malware detection.

Facebook: The company's license to store uploaded or shared content is broad, though users retain ownership of their data. Facebook can transfer licenses to other entities at any time and can share data with partners unless users manually opt out. If you share content with others, and then delete your account or specific files, shared files may not be deleted. The service provides extensive privacy settings for users to limit who can access their information.

Amazon: The company's Amazon Drive and Prime Photos products have a worldwide license similar to Google's, and its e-commerce site and hardware products store information in the cloud, including purchase histories. However, the TOS can be changed at any time without notice. Also, images will automatically be analyzed, tagged, and grouped by faces and locations. Image recognition can be disabled, though it is on by default.

Apple: The company's iCloud Drive and Photo Library TOS allows it to "prescreen" files, deleting content it finds "objectionable." For iPhone backups, if a device is not synced for 180 days, Apple can delete backups. Apple's Photo Library allows instantaneous sharing between selected individuals but it is important to note that deleting a file from your account does not automatically delete it from the devices of other authorized users. iCloud users will receive 30 days' notice before major TOS changes.

CSP privacy policies can vary and provide extensive rights to companies. Terms of Service Didn't Read (<https://tosdr.org/>) makes it easier to learn the privacy ins and outs of popular companies. The website provides a broad overview of the policies of CSPs and other online entities.



I, CLOUD: CREATE A PERSONAL CLOUD TO BALANCE SECURITY AND CONVENIENCE

In the cloud, consumers can have top-tier security or hassle-free convenience, but they cannot have both.

Security and convenience are inverse concepts; as one increases the other decreases. But with a rising number of data breaches, many users want more secure alternatives for cloud storage and services. From creating one's own cloud infrastructure—a complex feat advisable only for knowledgeable individuals—to using open-source software, users have several options to achieve greater privacy and security.

Security through obscurity: Technically-inclined individuals can set up private web servers to perform basic cloud functions: data storage and syncing. A user enables access to servers or network-attached (NAS) storage devices over a secure gateway. Though this cloud is private, it is wise to encrypt files before uploading. While few users can implement corporation-style security, the goal is security through obscurity. A cloud service with only one user is less of a target.


Zero knowledge: Zero-knowledge cloud services, such as Sync.com, encrypt data before it leaves your device.

Encryption keys are stored only on user devices, not servers, and companies cannot access data. File names and metadata are also encrypted and passwords are never stored on servers.

Private cloud: For a full-featured and secure private cloud service, try OwnCloud. The open-source, self-hosted solution manages calendars, contacts, and mail. Consumers install OwnCloud on private web domains and mobile apps keep data synced. Alternatively, OwnCloud can be used with commercial cloud providers, but this negates some privacy benefits. OwnCloud keeps encryption keys on servers, so users should encrypt files before uploading.

These solutions are not easy. Secure cloud storage is more difficult to use by design and you are responsible for keeping software updated, safeguarding passwords, and encrypting files. In the end, you must decide on the balance between convenience and security.

NEXT: Bring Your Own Umbrella



BRING YOUR OWN UMBRELLA: MANAGING CLOUD SECURITY RISKS

Your decision to use a cloud storage provider (CSP) should revolve around one question: can you trust the company?

Consumers should look for answers to specific questions regarding how the CSP implements security—within software and physical access to data centers—in which countries and jurisdictions it stores files and what regulatory schemes may apply, and the company's disaster recovery plan.

What encryption is used?

Not all CSPs provide specifics but, for those that do, consumers should determine if encryption protocols are tested by independent parties and deemed secure. Every encryption protocol has weaknesses so it is important how quickly a CSP patches flaws and bugs. Also, determine who controls encryption keys, the company or the consumer.

Where is data stored?

Where a CSP locates its data centers can affect privacy. Privacy laws vary greatly by country and some jurisdictions may allow government authorities or third parties easier access to data. If data centers are located outside of the United States, consumers should ensure they are in countries with strong data privacy laws, such as Iceland or Sweden. Avoid countries, such as India and China, that have weak privacy laws and are known to monitor CSP servers.

Is the CSP compliant with regulatory rules?

Depending on the jurisdiction, CSPs are subject to consumer protection laws, such as the Health Insurance Portability and Accountability Act of 1996, which protects access to health records, and European Union Safe Harbor, which controls how user data is transmitted from EU territories to the United States. The rules can change at any time, such as the European Union's new General Data Protection Regulation (GDPR) that takes effect in May 2018 and strengthens data protection

laws. Netskope's 2017 Cloud Report indicates that three-quarters of CSPs were not GDPR-ready.

How are facilities secured?

Learn how CSP facilities are physically protected from intrusions and employee misconduct. Review security procedures—at least the ones they will disclose—to determine if they meet your needs. For instance, RagingWire, a CSP in Virginia, uses iris recognition that detects if eyeballs are attached to living individuals before anyone can enter restricted areas. Amazon, which runs Amazon Web Services and is one of the largest CSPs, maintains a secure perimeter within and surrounding its data centers and requires two-factor authentication of staff, visitors, and contractors.

What is the disaster recovery plan?

A CSP with data centers in multiple countries has a level of redundancy built in. Copies of user data are maintained in two or more locations so if one data center faces a crisis, data may still be available at others. But consumers should review a CSP's specific data protection policies—what happens in the event of data loss, how many copies of user data are maintained and for how long, and can data be restored from partial backups?

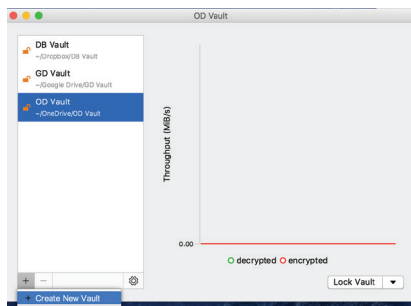
When it comes to the cloud, there is a great deal of information to consider. But educating yourself on how a CSP operates can help ensure your data is protected.

LOCK BEFORE YOU UPLOAD: HOW TO ENCRYPT DATA FOR THE CLOUD

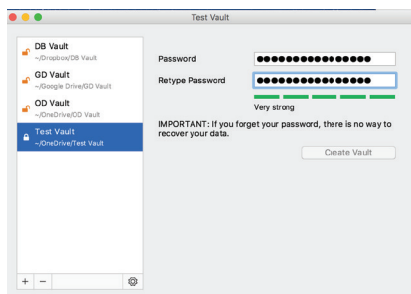
Encrypting files before uploading them to the cloud keeps them safe if your device is stolen, if your cloud account is compromised by hackers, or if the CSP itself wishes to view user files.

Of many cloud encryption solutions, Cryptomator provides more security because you do not need an account to use the app, it is open-source so its code can be reviewed, and it does not transmit any information to Cryptomator servers. It works for Windows, Macintosh, and Linux.

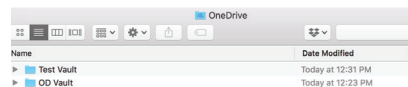
First, download the app from [Cryptomator.org](https://cryptomator.org). Once installed and launched, create a secure vault inside a CSP folder. Select the (+) button, create new vault, and navigate to the desired folder.



Give the vault a name and save. Cryptomator will prompt you to create a password. Select a secure password—at least eight characters with a mix of letters, numbers, and special characters—and save. Repeat these steps for each CSP folder. Store passwords in a safe place.



Your secure vault appears as a subfolder within your CSP folder.



Cryptomator mounts the vault as a virtual hard drive and opens a window to it. Files placed inside the vault are encrypted using AES with 256-bit keys—the same standard used by banks—and synced to the cloud. Folder and file names are also encrypted and the application obfuscates directory hierarchies, file types, and file sizes, though creation timestamps are still visible.

This is what you see:

Name	Date Modified	Size	Kind
catpic1.jpg	Today, 12:28 PM	946 KB	JPEG image
catpic2.jpeg	Today, 12:28 PM	5 KB	JPEG image
catpic3.jpeg	Today, 12:28 PM	5 KB	JPEG image
TextFile1	Today, 12:28 PM	178 bytes	RTF Document

This is what the cloud sees:

Name	Date Modified	Size	Kind
catpic1.jpg	Today, 12:28 PM	946 KB	JPEG image
catpic2.jpeg	Today, 12:28 PM	5 KB	JPEG image
catpic3.jpeg	Today, 12:28 PM	5 KB	JPEG image
TextFile1	Today, 12:28 PM	178 bytes	RTF Document

IMPORTANT: to encrypt files, they must be placed in the secure vault mounted by Cryptomator, NOT the unsecured vault folder visible in Finder (Mac) or File Explorer (PC).

To exit, select “lock vault” and close the application.

To access your cloud files, attackers would now need your CSP password and the password for your encrypted vault.

NEXT: Futures: Companies Can Face Major Fines...

GDPR

FUTURES: COMPANIES CAN FACE MAJOR FINES FOR LOSING YOUR DATA UNDER NEW EU REGULATION

A new European Union regulation will transform how cloud storage providers and other entities collect, store, and safeguard user data, providing consumers greater control over their personally identifiable information (PII).

The General Data Protection Regulation (GDPR), which becomes law in May 2018, imposes strict rules on entities, including US companies, that host or process PII of EU citizens. Non-compliant organizations face fines of up to 20 million Euros or 4 percent of revenues.

The United States has strong data protection laws, but its patchwork of federal and state regulations allows for gaps in protection. A company can avoid privacy laws in one place by basing operations in another state or country.

Under GDPR, organizations must:







- Get affirmative consent to collect, process, or share PII. Companies must clearly state what data is collected, why it is requested, how it is used, and with whom it is shared. Consumers must receive clear options to withdraw consent and delete data.
- Protect PII, including name, address, sexual orientation, IP address, location, and cookie data. Explicit permission

is required for sensitive information: race, medical, biometrics, union membership, and political opinions.

- Disclose data breaches within 72 hours and whenever PII is transferred to or stored in another country.
- Provide consumers downloadable versions of data in formats that can be shared with other entities.
- Implement safeguards, such as encryption or pseudonymization.

The short-term impact of GDPR is unclear. Most companies are unlikely to meet the deadline, but it is unknown how heavy-handed regulators will be early on. Additionally, US consumers may not benefit as companies could isolate data on EU citizens while maintaining lax protections for others. However, US companies likely will implement uniform policies rather than risk mishandling PII of EU citizens who use services while traveling.

Popular Cloud Service Providers

	CLOUD SERVICES	DATA CENTER LOCATIONS	ZERO-KNOWLEDGE PROOF	ENCRYPTION IN TRANSIT/ AT REST	END-TO-END ENCRYPTED/ FILE STORAGE	REMOTE DEVICE WIPE	HIPAA-COMPLIANT?
	storage, virtual computing, database management	United States, Australia, Brazil, China, European Union, India, Japan, Singapore, South Korea	✗	✓✓	✗✗	✗	✓
	storage, messaging, video chat, email, VOIP	United States, China, European Union, Singapore	✗	✓✓	✗✗	✓	✓
	storage	United States, European Union	✗	✓✓	✗✗	✓	✓
	storage, messaging, video chat, email, VOIP	United States, European Union, Singapore, Taiwan	✗	✓✓	✗✗	✓	✓
	storage, messaging, video chat, email, VOIP	United States, Brazil, China, European Union, India, Japan, South Korea	✗	✓✓	✗✗	✗	✓
	storage, messaging	United States	✓	✓✓	✓✗	✗	✓
	storage	European Union	✓	✓✓	✓✓	✓	✓

For more detailed information on protecting and managing other key elements of your identity footprint online please check out the Identity Awareness, Protection and Management Guide.

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE
COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS
SIXTH EDITION, MARCH 2018



BROUGHT TO YOU BY:



U.S. DEPARTMENT OF DEFENSE

Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL

CLOUD
COMPUTING