

April 2023

Using encryption to secure government data and digital services

Offered to Apolitical members



Internet Society
encryption@isoc.org

How governments are using encryption
How encryption can help protect your government
How your government can start using encryption



A responsible government will use encryption to protect government and citizens' data.



Encryption secures data



Use encryption to secure

- internal and external communications
- documents, data and e-govt services
 - especially personal, sensitive, confidential, classified data
- **government ➤ citizens**
 - e.g. official announcements and information
- **citizens ➤ government**
 - e.g. citizen complaints and crime reporting
- investigations, evidence and judicial proceedings
- archives, IoT, smart cards ...



Photo by [Ula Kuźma](#) on [Unsplash](#)



Use encryption to
protect data
integrity

“ ... any potential for data
to be modified undetected
may affect the reliability
of the reports created and
... may result in the evidence ...
being rendered inadmissible.”

Use encryption to protect
citizen to government
transactions



Photo by [Brett Jordan](#) on [Unsplash](#)



in use, in transit, at rest



Photos by [Gary Bendig](#), [Vincent van Zalinge](#) and [Grant Durr](#) on [Unsplash](#)

Data in transit

- end-to-end encryption
 - only the sender and receiver can read the contents of the message
 - think of it as “**person-to-person encryption**”
- channel encryption
 - service provider could and may read (and use!) the contents

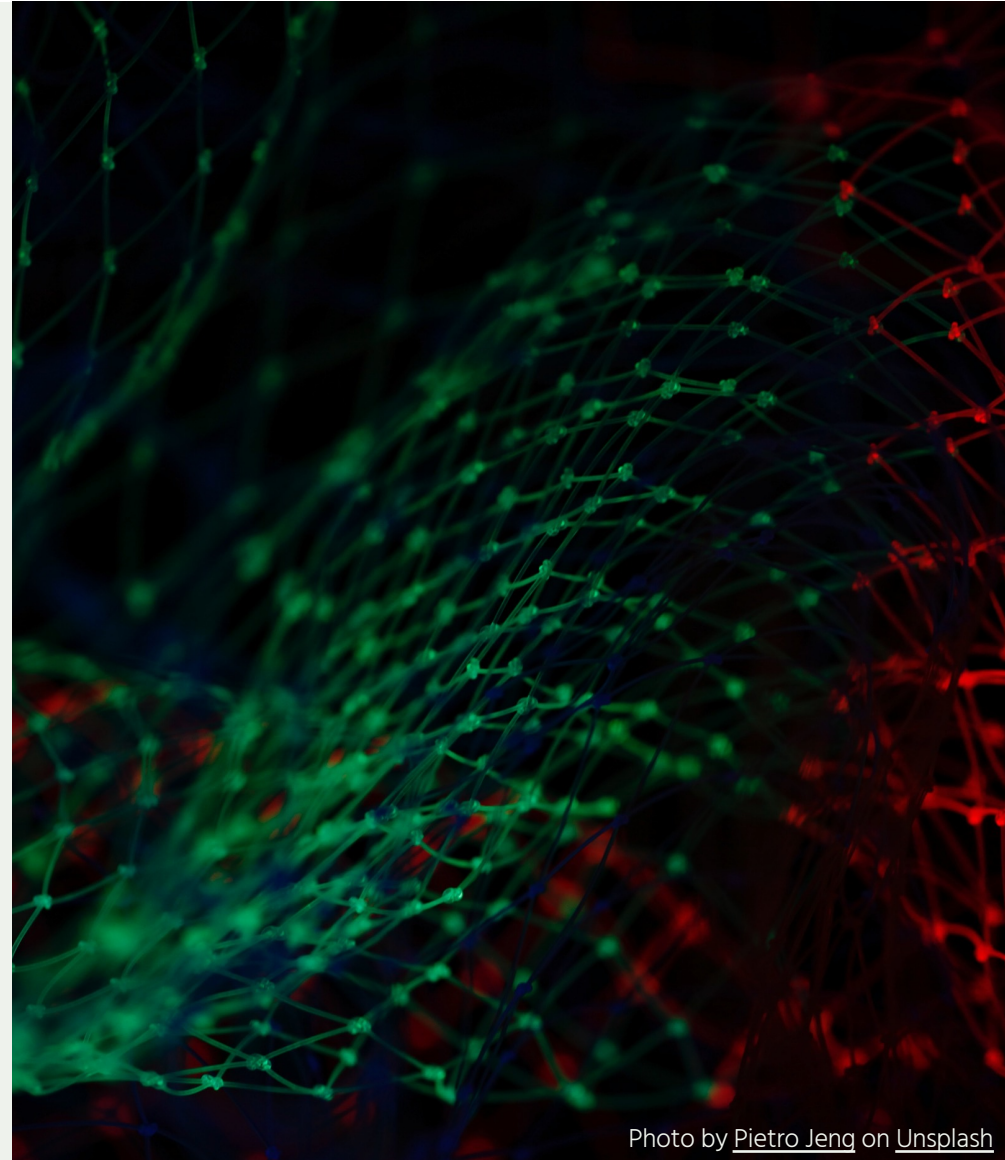


Photo by [Pietro Jeng](#) on [Unsplash](#)

Data at rest

- user-controlled encryption
 - only the user has the key to decrypt the files
 - also called “zero-knowledge encryption”
 - examples: Mac OS FileVault, Windows BitLocker, iOS, Android
- service-controlled encryption
 - the service has the ability to decrypt the files
 - examples: Google Drive, some data categories of iCloud backups, Box, Dropbox



Photo by [Denny Müller](#) on [Unsplash](#)

Data in use

- Don't leave devices unlocked or unattended, not even for a moment



Websites and web services

- **HTTPS-only policy** - some governments require all government websites and web services to only use HTTPS
- They also often require:
 - re-direct from HTTP
 - disable known weak protocols (such as SSL, TLS 1.0 and 1.1)
- **Note:** a partially encrypted website is vulnerable to MITM attacks (check that all elements are loaded over HTTPS)
- Use **HTTPS-only mode** in web browsers



Photo by [Nick Fewings](#) on [Unsplash](#)

Stored documents and data

- Securely encrypt stored documents and data to:
 - satisfy privacy and data protection law data security requirements (compliance)
 - limit disclosure if breached (mitigation)
- **Power down devices** when not in use
- **Note:** the data on encrypted disks, drives or devices is not generally encrypted while they are in use
- Create “**encryption nests**” to protect data on an encrypted disk, drive or device
- Limit who has access and use 2FA



Photo by [m](#) on [Unsplash](#)

Backups

- Encrypt locally before backing up to the cloud
- Note: If an encrypted cloud service does not use “user-controlled encryption” the service provider is able to reverse the encryption (and read the contents)
- Isolate recovery backups from the Internet
- Have a disaster recovery plan for your data



Photo by [C Dustin](#) on [Unsplash](#)

Why applying encryption correctly is important

Table from “Some Privacy Practices May Result in Under-Reporting of Breach Incidents” by Kelce S. Wilson, CIPP/E, CIPP/US, CIPM published by the International Association of Privacy Professionals (IAPP)

https://iapp.org/media/pdf/resource_center/Encryption-Exception-Breach-Report-Whitepaper-FINAL.pdf

- Best practice:
 - don't store the key with the encrypted data
 - require a physical action to cause decryption



Method of Compromise	Encryption Scenario			
	Encrypted data is accessible by a processor and software application that operates on it in cleartext form.		Encrypted data is not accessible by a processor or software application that operates on it in cleartext form.	
	A. Key material is accessible by a processor and automatically decrypts data for use by software. Common	B. Key material is not accessible by a processor until physical action decrypts data for use by software. Common	C. Key material is accessible by the same network on which the data is archived.	D. Key material is not accessible by same network on which data is archived, but is kept physically separate.
1. Data and key are both stolen at the same time.	Vulnerable; easy to decrypt	Prevented	Vulnerable; easy to decrypt	Prevented
2. Data and key are stolen in same compromise, different times.	Vulnerable to a persistent threat	Vulnerable to a persistent threat	Vulnerable to a persistent threat	Prevented
3. Data is stolen when it is used by software in cleartext form.	Vulnerable; timing is important	Vulnerable; timing is important	Prevented	Prevented
4. Data and key are stolen separately in different incidents.	Vulnerable; possibly delayed compromise	Vulnerable; possibly delayed compromise	Vulnerable; possibly delayed compromise	Vulnerable; possibly delayed compromise
5. Encryption is weak; less than 256 bit.	Vulnerable; easy to decrypt	Vulnerable; easy to decrypt	Vulnerable; easy to decrypt	Vulnerable; easy to decrypt
6. Password is weak; under 15 characters.	Vulnerable; easy to decrypt	Vulnerable; easy to decrypt	Vulnerable; easy to decrypt	Vulnerable; easy to decrypt
7. Sophisticated attack limits key entropy, permits guessing of key.	Vulnerable; advanced stealth threat	Vulnerable; advanced stealth threat	Vulnerable; advanced stealth threat	Vulnerable; advanced stealth threat

Passwords

The best encryption in the world will not protect you if your passwords and password management practices are poor.

- password complexity is good
- do not re-use passwords
- use a trusted password manager
- use multi-factor authentication
- delete and disable inactive accounts
- limit who has access
- monitor breaches
- remove personal data from data brokers
- don't use real info to answer security questions

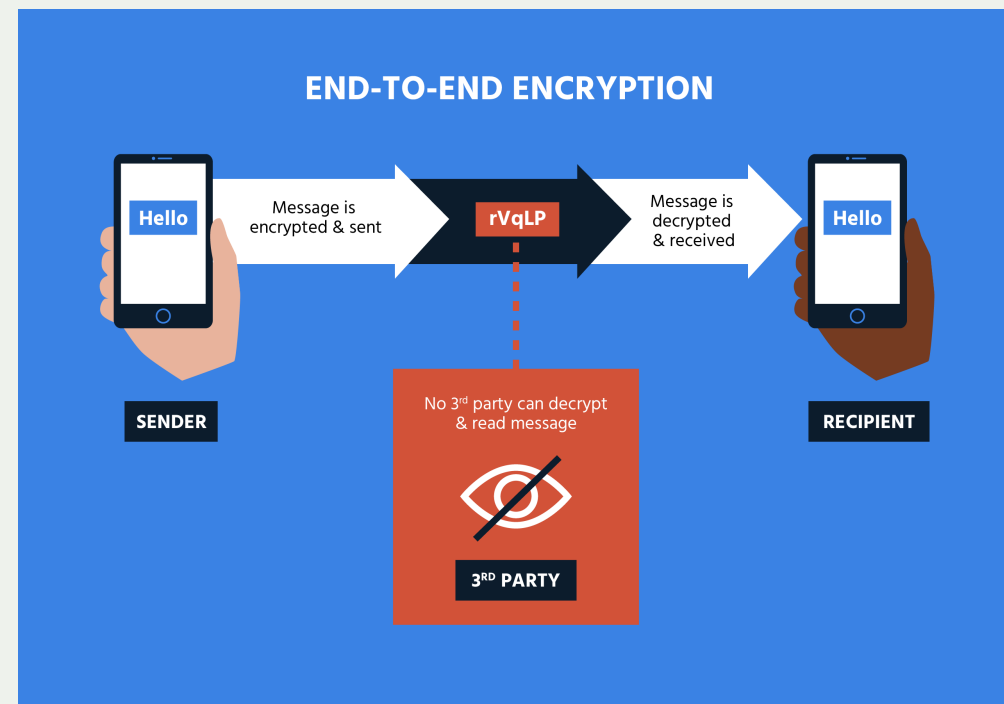


Messaging apps



Messaging apps (data in transit)

- **End-to-end encryption only policy** – some governments and institutions require officials to use messaging services that use end-to-end encryption
 - European Commission (use Signal)
 - Colombia government agencies of the national executive branch (use e-2-e)
 - US Senate (use Signal)
 - US 82 Airborne Task Force Devil Unit (use Signal or Wickr)



Communicating trusted information about COVID-19 using end-to-end encryption

- **WHO** Health Alert (uses WhatsApp)
- **India** MyGov Corona Helpdesk WhatsApp chatbot
- **Australia** government WhatsApp channel for COVID-19
- **Singapore** Gov.sg WhatsApp
- **UK Gov.**UK Coronavirus Information Service on WhatsApp
- **Niger** WhatsApp chatbot
- **City of Buenos Aires** (Boti) WhatsApp chatbot

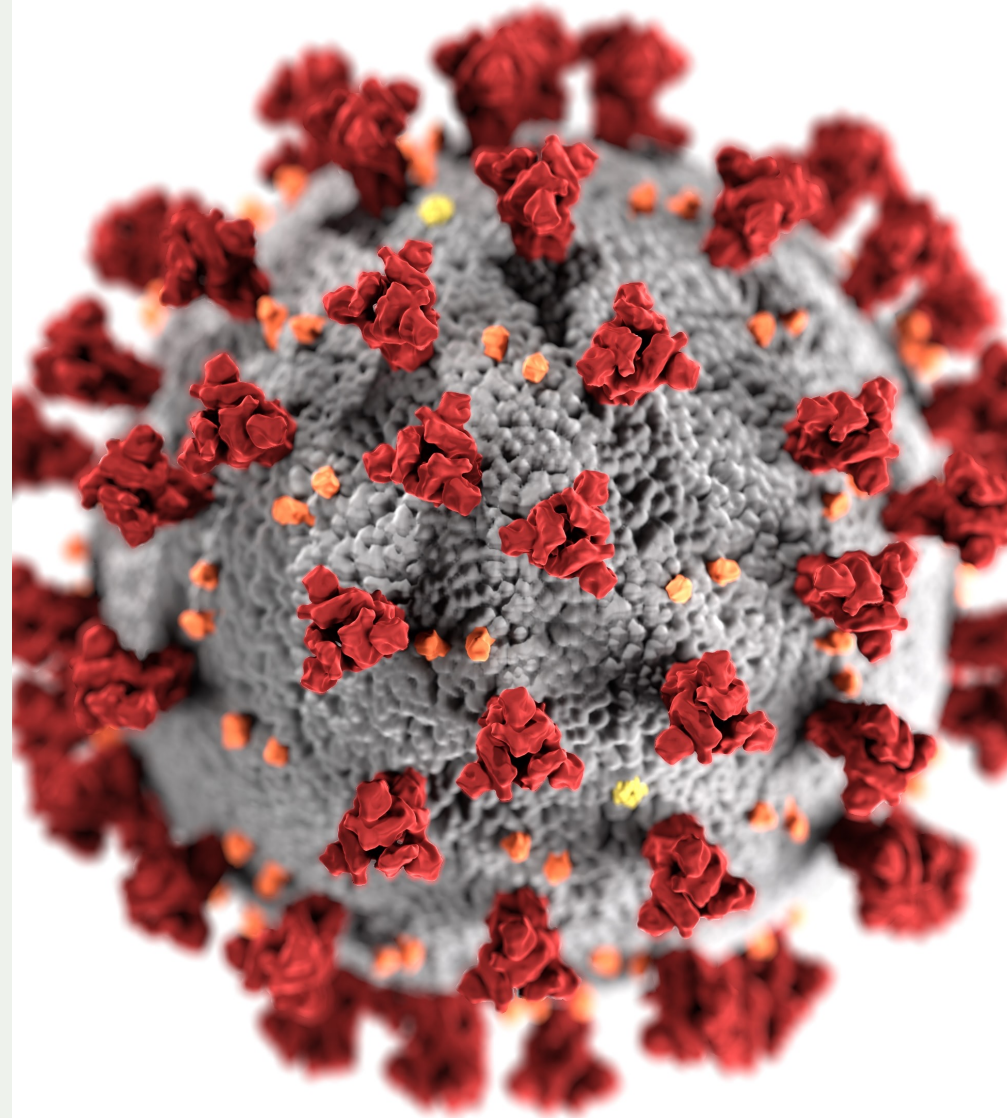


Photo by [CDC](#) on [Unsplash](#)

Helping citizens report crimes confidentially and securely

- **Kolkata** Police WhatsApp helpline for cyber and petty crime reporting (India)
- **Bhubaneswar** Police WhatsApp number for crime reporting (India)
- Royal **Malaysian** Police WhatsApp channel regarding commercial crimes for Commercial Crime Investigation Department



Photo by [David von Diemar](#) on [Unsplash](#)

Some future trends

- password-less authentication (also known as passkeys)
- secure multi-party computation
- post-quantum technology



Photo by [drmakete lab](#) on [Unsplash](#)

Considerations when using end-to-end encryption



Choose a well-regarded service

- choose a service that has been checked by security researchers
 - correctly implementing encryption, particularly for multi-party conversations, is not straightforward
 - trying to build your own encryption system is a bad idea
 - no cryptographer would recommend that approach

Forbes

Apr 20, 2019, 06:29am EDT | 5,699 views

French Government's 'Secure' WhatsApp Replacement Hacked In Just 90 Minutes

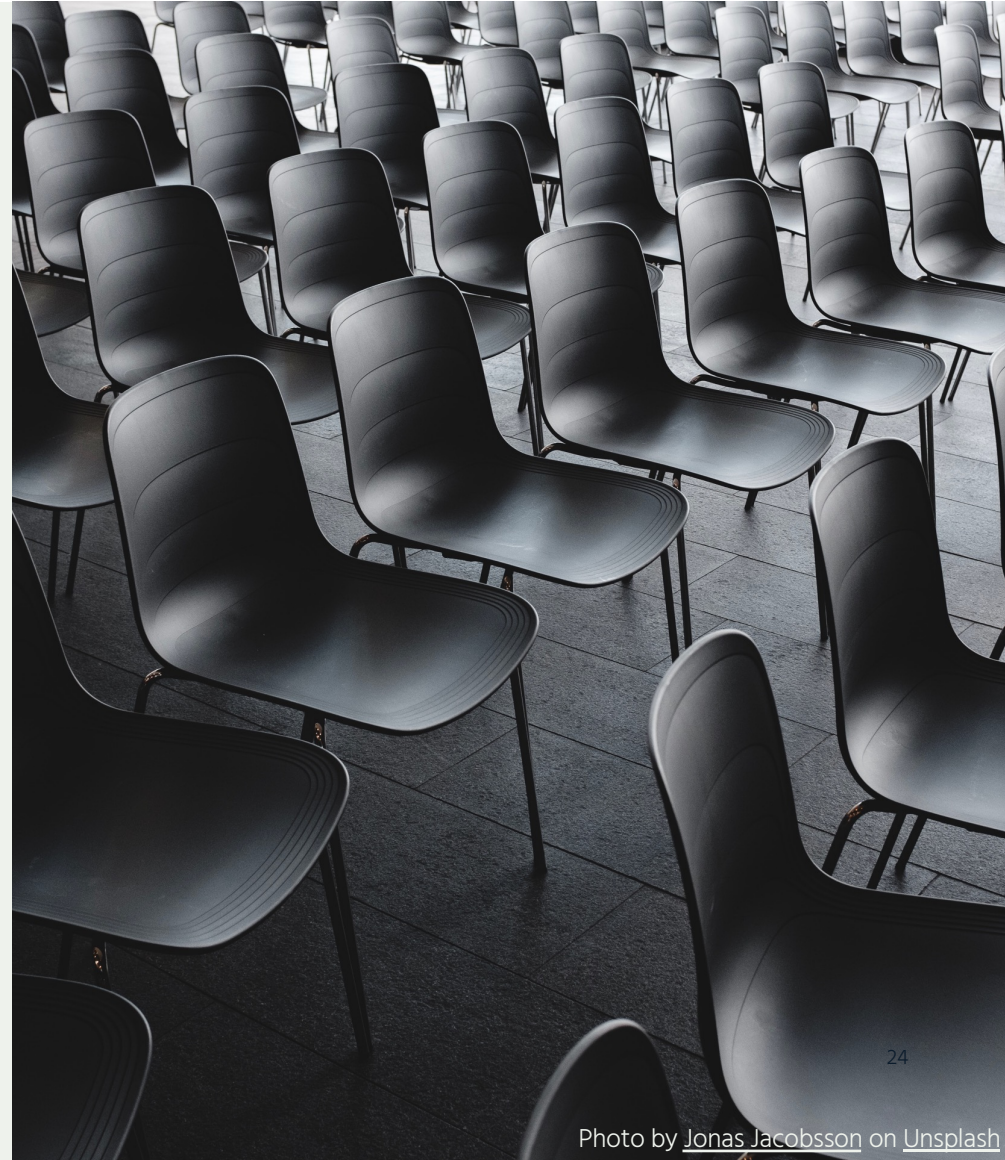


Join Extra Crunch

Security flaw in French government messaging app exposed confidential conversations

Consider your audience

- popular end-to-end encrypted messaging apps are not interoperable
- What services are your audience already using?
- a “boutique” app designed for internal government use is unlikely to be interoperable with externally used apps



Make sure encryption is on by default

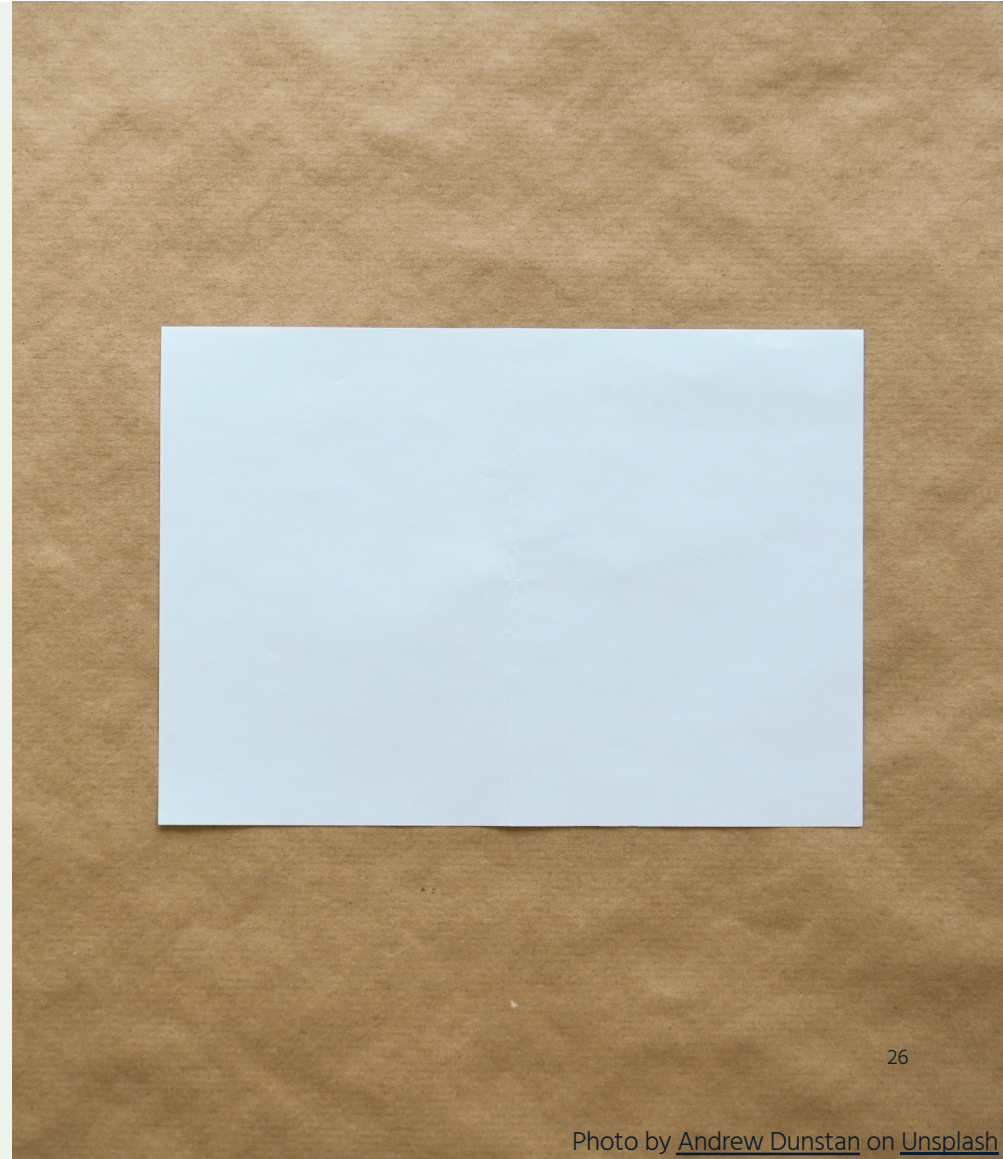
- only some messaging services offer end-to-end encryption
- users are notoriously bad at changing default settings
- choose a service that has end-to-end encryption on by default, so users do not accidentally send an unencrypted communication (big oops!)



Photo by [Becky Phan](#) on Unsplash

Choose a service that minimizes metadata exposure

- read the privacy policy carefully before choosing a service.
- pay attention to what metadata is exposed and how it will be used by the service.
- examine what personal data the service collects as part of the service and from other sources (such as data brokers).



Make sure backups are secure

- backups are an important aspect of proper official records management
- backups should be stored in an encrypted format
- if you use an external cloud storage service for backups, make sure they cannot decrypt the backup
- only authorized users should have the keys to decrypt the backup



Photo by [Thomas Jensen](#) on [Unsplash](#)

Have a policy regarding use of the “disappearing message” feature

- use of “disappearing message” feature could raise questions about government transparency and conduct, and could be a violation of official records requirements



Photo by [Brandon Duford](#) on [Unsplash](#)

Consider what is appropriate use and how records management policies apply

- information may need to be disclosed in the future, such as for legal proceedings, pursuant to a Freedom of Information or privacy law request, or because a public access period has started.
- It is imperative to have clear and enforceable guidelines on the appropriate use of these services and their records management



Photo by [C M](#) on [Unsplash](#)

Does the definition of an official record need to be updated?

Director General David Fricker of the National Archive of Australia:

The Archives Act defines a commonwealth record as being a record that is the property of the Commonwealth. WhatsApp is not the property of the commonwealth; Facebook is not the property of the commonwealth”

<https://www.themandarin.com.au/153988-encrypted-messages-are-grey-area-in-record-keeping-requirements-david-fricker-says/>



Implications of using a commercial service for government use

- What if the service goes down or ceases to exist?
- What if the service is located outside your jurisdiction?
- What if a court or another part of government orders access to the app to be blocked?
- What if app stores suspend or remove the app?



question

What change are you going to make at work to ensure your documents, data and/or communications are more secure?



Thank you.

Internet Society
encryption@isoc.org



Rue Vallin 2
CH-1201 Geneva
Switzerland

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

66 Centrepont Drive
Nepean, Ontario, K2G 6J5
Canada

Science Park 400
1098 XH Amsterdam
Netherlands

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internet society.org
@internetsociety