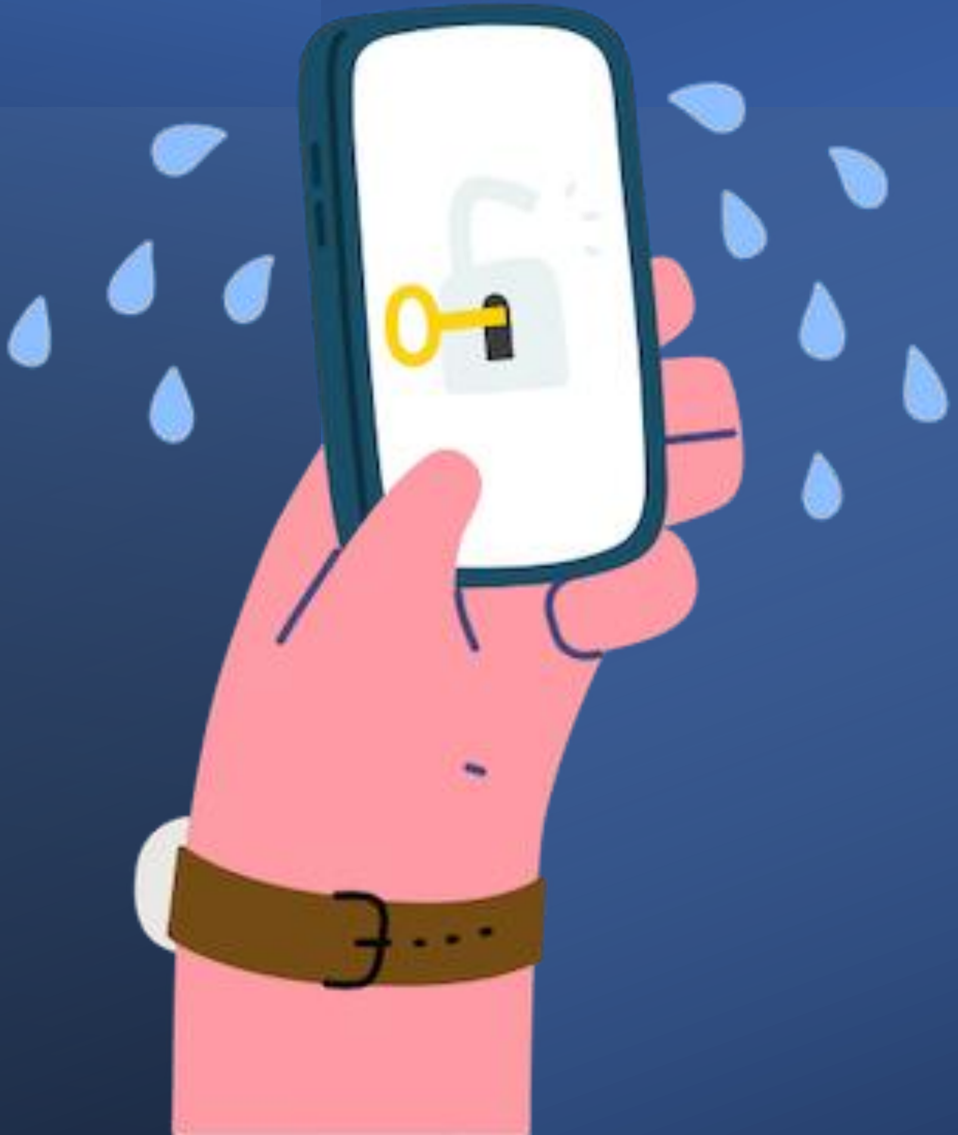
J **I** Y u ä
o 8 ₹ e #
7 γ **G** 7 ø
ω € H 3 9
R D ÿ h **T**
$ ƒ @ $ η
T r 5 **H** $
S & 2 % ;

to

π i ξ u **A** D a
1 8 **l** e # p g
P s G 5 U ß ğ
H E $_2$ 3 h A Æ
r **R** R **V** T ^{6} þ
@F k \$ h **C**$_3$
T a 5 H ů $ x
v - 2 %o ; **Y**



o 3 #

7 Y h ø

ω ₹ $ 9

R I G H T

$ 8 H % η

T γ ÿ $

S € @ ;

D 5

ʃ 2

r

&

to

8 e ß ƀ

π s 5 A 3

1 E ξ 3 6 x

PRIVACY

H F G$ # $

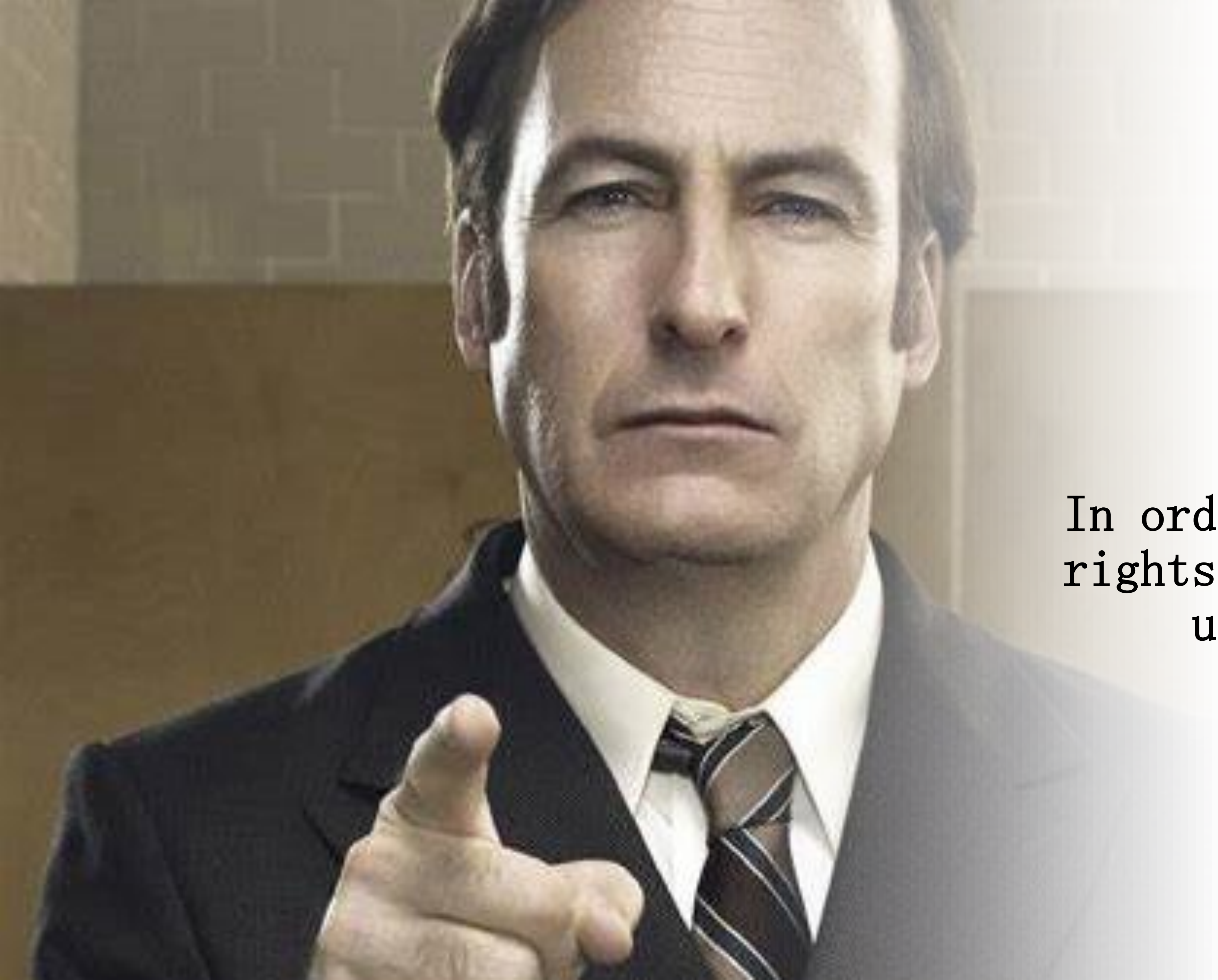
r a 2 H U ;

@- R% h

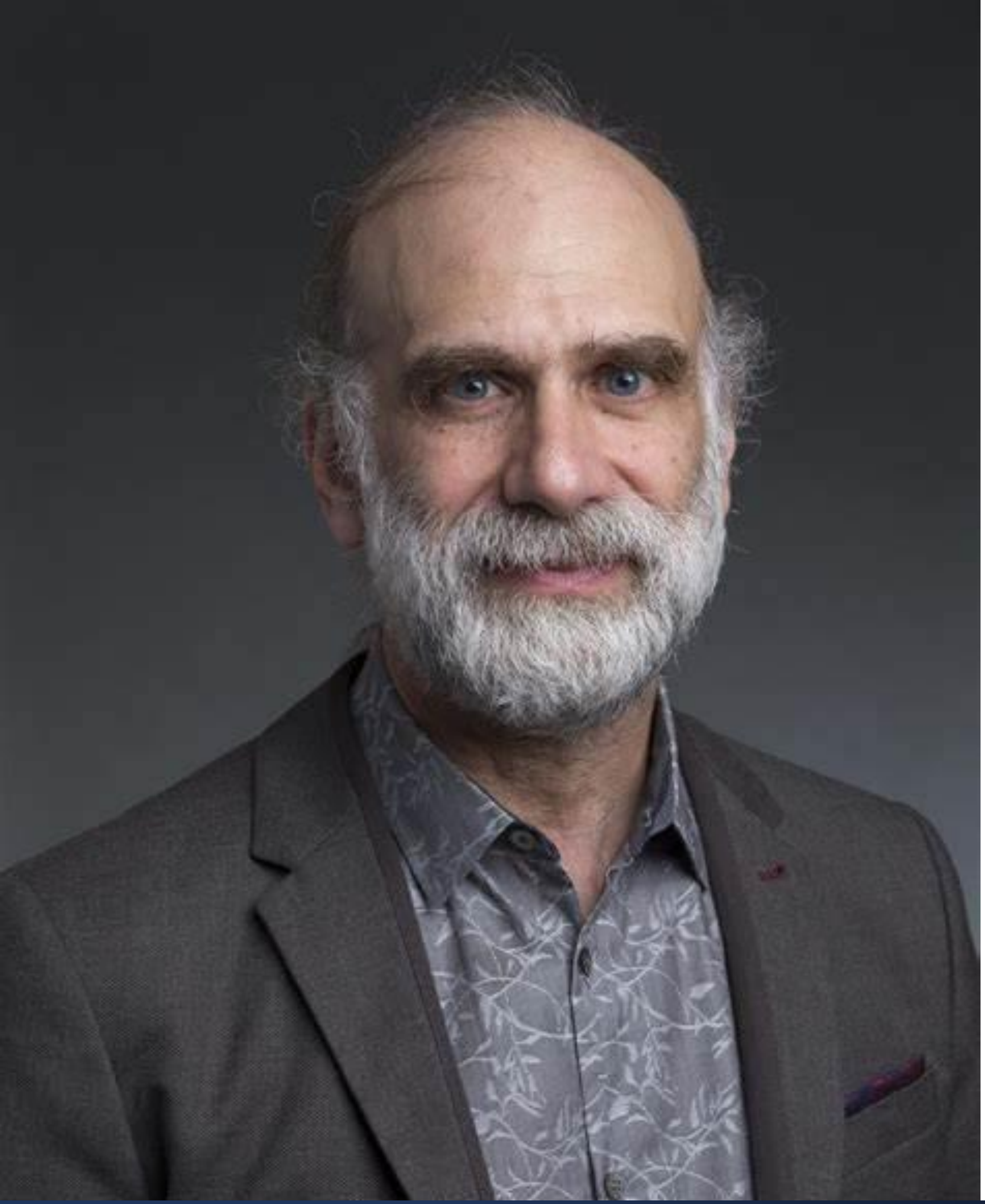
T k T

v 5 h

2 ů



In order to exercise your rights, you must know and understand them

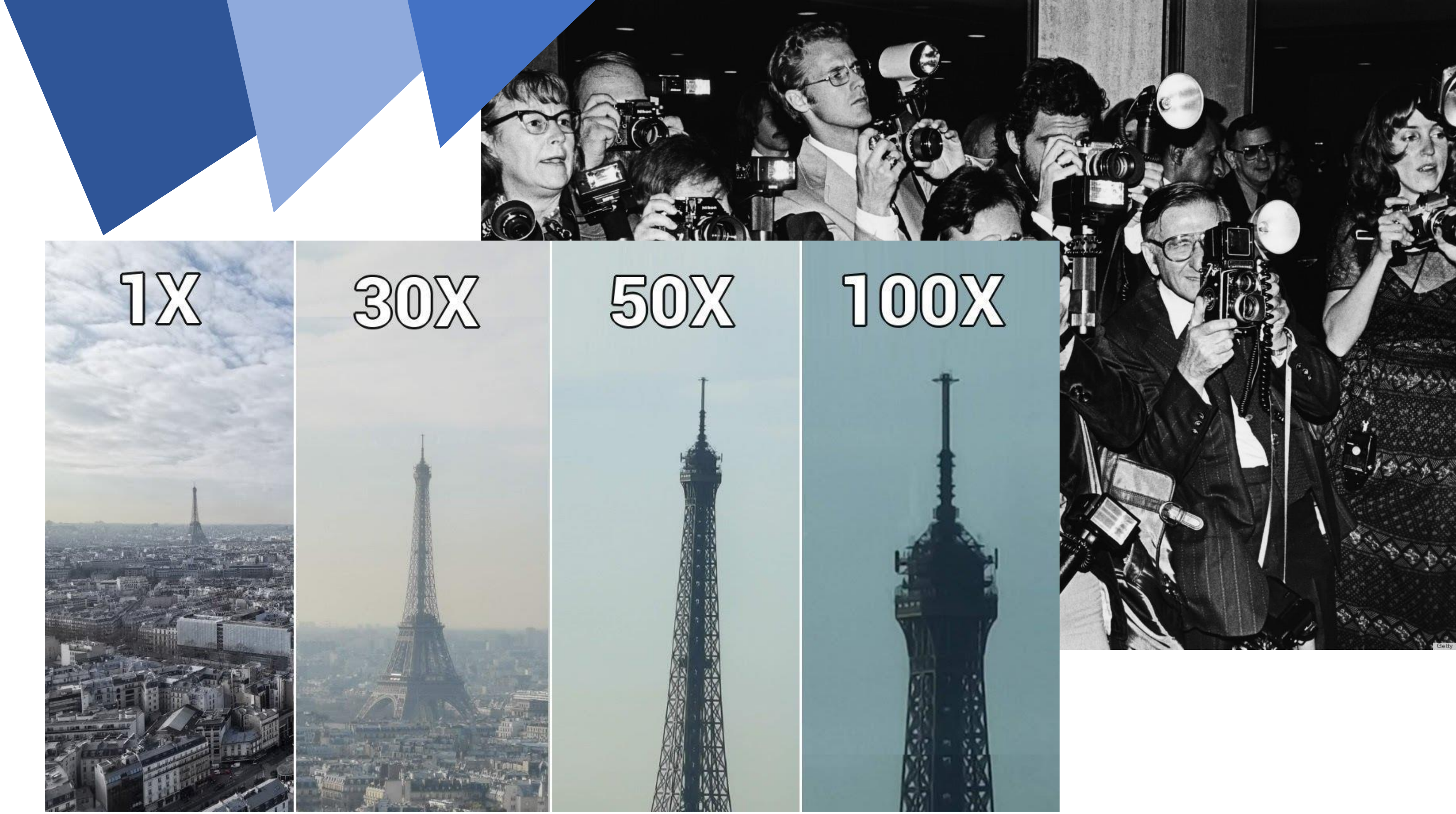


"Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance."

Bruce Schneier

Our smartwatches and smartphones gather information continuously

Most of our smartphones are able to recognize our faces and our fingerprints

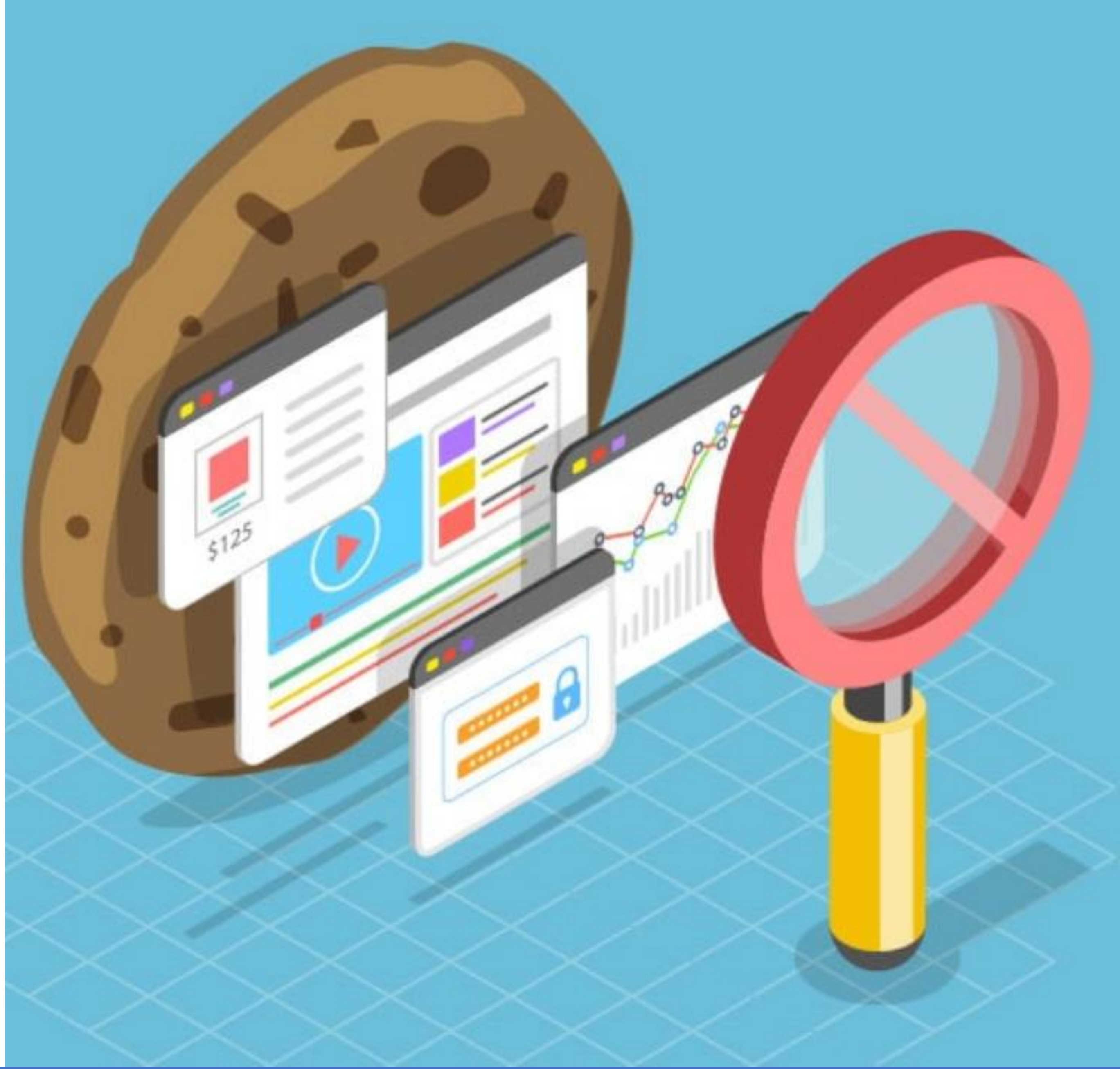


The new Samsung S23 Ultra as an example: its lenses have a maximum magnification power of x100

We leave behind us a trace of data that is nearly impossible to recover or even delete once it sets adrift on the internet: our DIGITAL FOOTPRINT.

Cookies: a fundamental instrument for web browsers to enhance the user experience.

Tracking cookies, also known as third-party cookies, gather our activity and web habits adding them to our personal footprint



"If something is free then you are the product"

General
Data
Protection
Regulation

The GDPR is one of the strictest and most complete laws regarding data privacy and security of European Citizens. It’s a document of hundreds of pages in itself so it is large, far-reaching and fairly light on specifics; it establishes sanctions and penalties that can reach into the tens of millions of euros.

Privacy enables us to create boundaries and protect ourselves from unwarranted interference in our lives, allowing us to negotiate who we are and how we want to interact with the world around us.

Violation of privacy

The Chinese government has created a "Police Cloud" system that tracks and predicts the activities of activists, dissidents, and ethnic minorities, including those with "extreme thoughts".

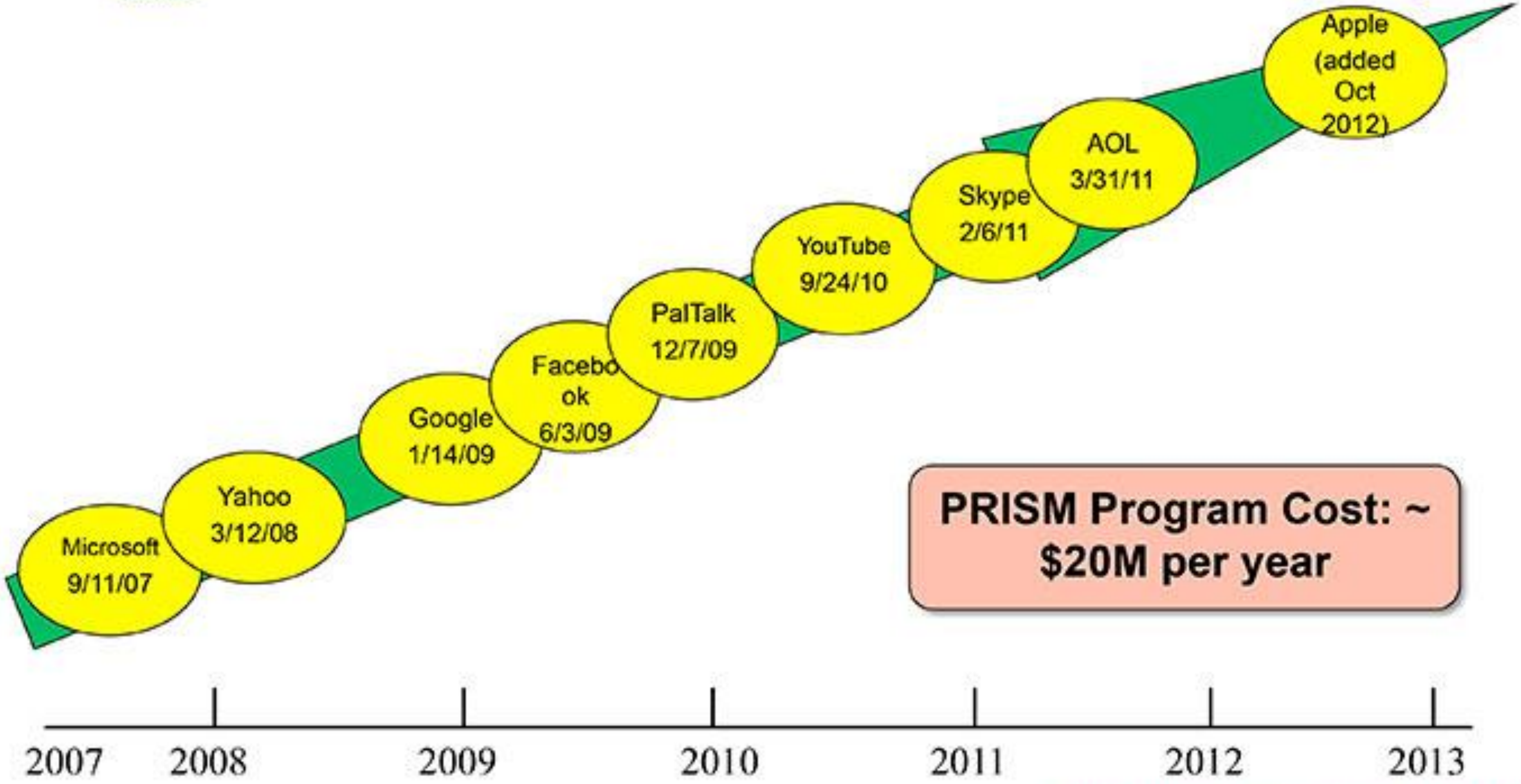
China is using facial recognition technology to track ethnic minorities, even in Beijing. Xinjiang authorities have increased mass surveillance measures across the region, augmenting existing tactics with the latest technologies

Edward Snowden

"Saying you don't care about privacy because you've got nothing to hide is like saying you don't care about freedom of speech because you have nothing to hide"

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

In 2012, it was revealed that the FBI had monitored the Occupy Wall Street movement in the United States, using counterterrorism agents and other resources.

The FBI treated the Occupy movement as a potential criminal and terrorist threat, and FBI offices and agents around the country were involved in monitoring the group, despite the protests being pacific.

LEAs also make extensive use of social media to track down/identify people who take part in protests or even just suspected protesters. They gather thousands of videos and pictures available online and then scan them using facial recognition technology. To accomplish this, they sometimes use tools like Clearview AI, a tool that has been part of a controversy recently for downloading without permission tens of billions of pictures from social media in order to catalog them based on biometric data and make it readily available to LEAs.

FEDERAL BUREAU OF INVESTIGATION

LAWFUL ACCESS

(U//FOUO) FBI's Ability to Legally Access Secure Messaging App Content and Metadata

(U//LES) As of November 2020, the FBI's ability to legally access secure content on leading messaging applications is depicted below, including details on accessible information based on the applicable legal process. Return data provided by the companies listed below, with the exception of WhatsApp, are actually logs of latent data that are provided to law enforcement in a non-real-time manner and may impact investigations due to delivery delays.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

App	iMessage	Line	Signal	Telegram	Threema	Viber	WeChat	WhatsApp	Wickr
Information Accessed	SUBSCRIBER DATA DEVICE BACKUP MESSAGE SENDER-RECEIVER DATA USER'S CONTACTS DATE/TIME INFORMATION REGISTRATION TIME DATA ENCRYPTION KEY(S)	SUBSCRIBER DATA MESSAGE SENDER-RECEIVER DATA USER'S CONTACTS DATE/TIME INFORMATION REGISTRATION TIME DATA	REGISTRATION TIME DATA DATE/TIME INFORMATION	REGISTRATION TIME DATA	SUBSCRIBER DATA REGISTRATION TIME DATA DATE/TIME INFORMATION ENCRYPTION KEY(S)	SUBSCRIBER DATA DATE/TIME INFORMATION IP ADDRESS ENCRYPTION KEY(S) REGISTRATION TIME DATA	SUBSCRIBER DATA REGISTRATION TIME DATA IP ADDRESS	SUBSCRIBER DATA REGISTRATION TIME DATA MESSAGE SENDER-RECEIVER DATA USER'S CONTACTS DATE/TIME INFORMATION	SUBSCRIBER DATA REGISTRATION TIME DATA DATE/TIME INFORMATION
Legal Process & Additional Details	• **Message Content: Limited** • **Subpoena:** can render basic subscriber information • **18 U.S.C. §2703(d):** can render 25 days of iMessage lookups to and from a target number[3] • **Pen Register:** no capability[3] • **Search Warrant:** can render backups of a target device; if target uses iCloud backup, the encryption keys should also be provided with content return; can also acquire iMessages from iCloud returns if target has enabled Messages in iCloud	• **Message Content: Limited*** • Suspect's and/or victim's registered information (profile image, display name, email address, phone number, LINE ID, date of registration, etc.) • Information on usage *Maximum of seven days' worth of specified users' text chats (Only when E2EE has not been elected and applied and only when receiving an effective warrant; however, video, picture, files, location, phone call audio and other such data will not be disclosed)	• **No Message Content** • Date and time a user registered • Last date of a user's connectivity to the service	• **No Message Content** • No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram *may* disclose IP address and phone number to relevant authorities	• **No Message Content** • Hash of phone number and email address, if provided by user • Push Token, if push service is used • Public Key • Date (no time) of Threema ID creation • Date (no time) of last login	• **No Message Content** • Provides account (i.e. phone number) registration data and IP address at time of creation • Message History: time, date, source number and destination number	• **No Message Content** • Accepts preservation letters and subpoenas, but cannot provide records for accounts created in China • For non-China accounts, they can provide basic information (name, phone number, email, IP address), which is retained for as long as the account is active	• **Message Content: Limited*** • **Subpoena:** can render basic subscriber records • **Court Order:** Subpoena return as well as information like blocked users • **Search Warrant:** Provides address book contacts and WhatsApp users who have the target in their address book contacts • **Pen Register:** Sent every 15 minutes, provides source and destination for each message *If target is using an iPhone and iCloud backups enabled, iCloud returns may contain WhatsApp data, to include message content	• **No Message Content** • Date and time account created • Type of device(s) app installed on • Date of last use • Total number of messages • Number of external IDs (email addresses and phone numbers) connected to the account, but not plaintext external IDs themselves • Avatar image • Limited records of recent changes to account setting such as adding or suspending a device (does not include message content or routing and delivery information) • Wickr Version Number

SUBSCRIBER DATA · MESSAGE SENDER-RECEIVER DATA · DEVICE BACKUP · IP ADDRESS · ENCRYPTION KEY(S) · DATE/TIME INFORMATION · REGISTRATION TIME DATA · USER'S CONTACTS

(U) Prepared by Science and Technology Branch and Operational Technology Division

7 January 2021

[3] (U//LES) Apple provided logs only identify if a lookup occurred. Apple returns include a disclaimer that a log entry between parties does not indicate a conversation took place. These query logs have also contained errors.

(U) LAW ENFORCEMENT SENSITIVE: The information marked (U//LES) in this document is the property of FBI and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.

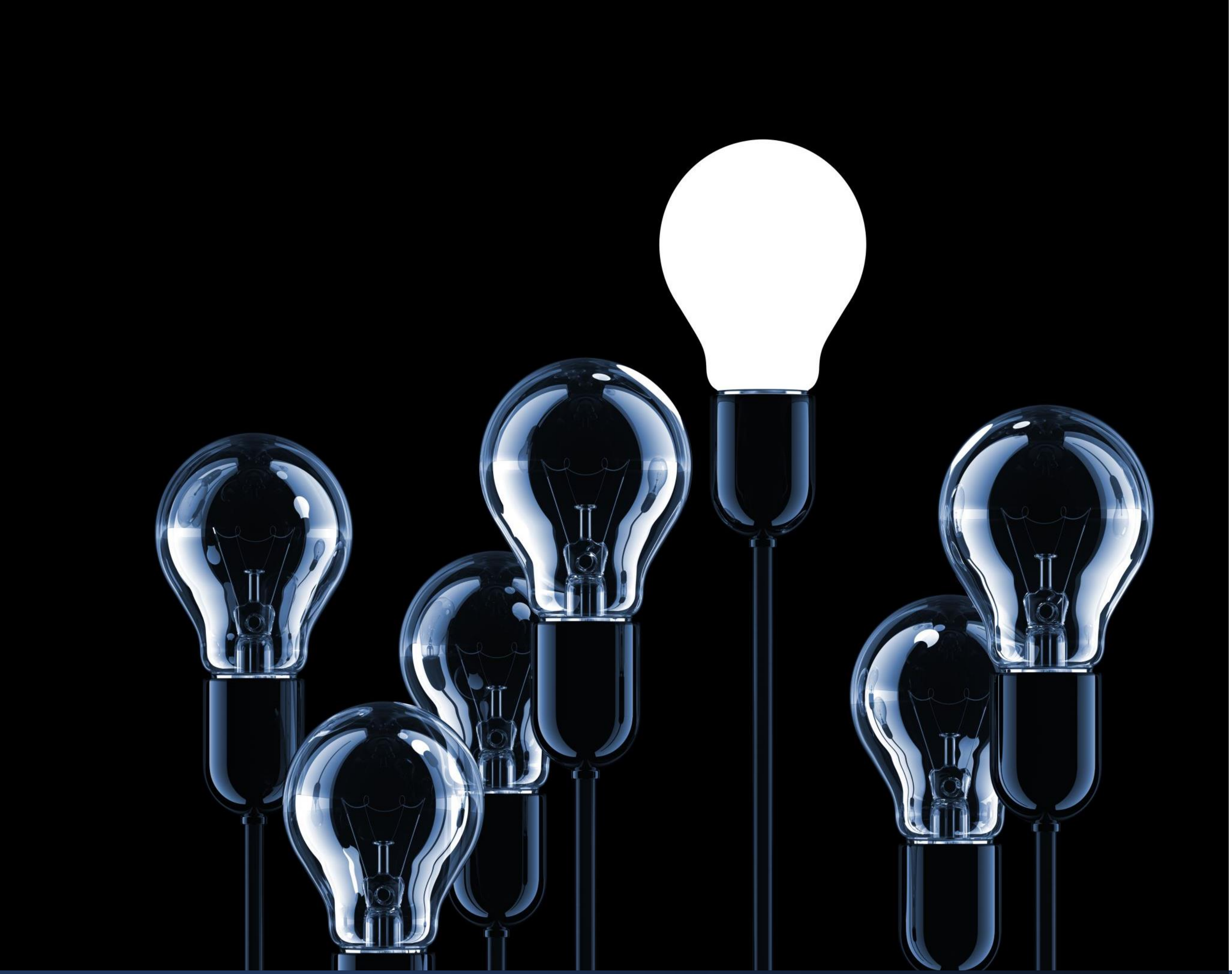
DEBATE

If you had the chance,
would you ever break someone's privacy to gather information on them?

Do you value your privacy enough?

Are you fine with your data being sold
to anyone?

Can mass surveillance be justified
in some cases?



THANK YOU FOR YOUR ATTENTION

Cocino Gabriele
Eirale Emanuele
Marengo Giulia