TICT 3142 Social and Professional Issues in IT

Lesson 05 Privacy

T. Nusky Ahamed
Lecturer (Prob)
Department of ICT
Faculty of Technological Studies
University of Vavuniya

🔐 1. Introduction to Privacy in ICT

- Privacy in ICT refers to the ability of individuals and organizations to control the collection, use, and dissemination of personal or sensitive information.

Importance:

- With the widespread use of digital technologies, individuals constantly generate data (e.g., browsing history, location data, communications).
- Without adequate privacy protections, this data can be misused for identity theft, surveillance, or unethical profiling.

Types of Privacy

Informational Privacy: Ensures control over how personal data (e.g., medical records, financial data) is collected, stored, and shared.

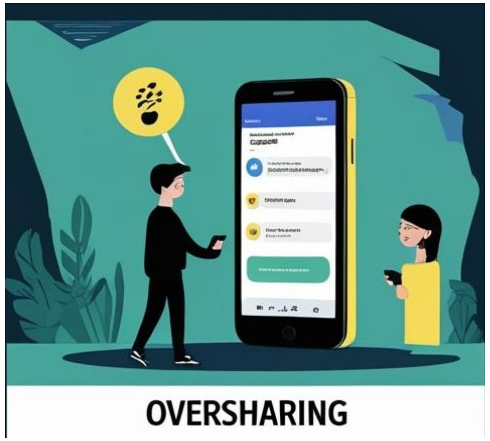
Bodily Privacy: Protection against invasive procedures or biometric data collection (e.g., fingerprints, retina scans) without consent.

Territorial Privacy: The right to maintain the privacy of personal spaces such as homes, offices, or digital storage.

Communication Privacy: Safeguards emails, phone calls, and messages from unauthorized access or interception.

👥 2. Social Aspects of Privacy

🔐 Social Media Privacy



Oversharing Risks: Many users share birthdays, locations, relationships, travel plans, and personal opinions often unaware of how this information might be used maliciously.

Manipulative Design: Platforms use dark patterns to make privacy settings hard to access or confusing, nudging users to expose more data.

Data Breaches: Hacks and leaks (like the Facebook–Cambridge Analytica scandal) can expose millions of users' private data.

Third-Party Access: Social media platforms often share user data with advertisers, app developers, and sometimes even law enforcement, with or without proper user consent.

🆔 Online Identity and Anonymity

Real Identity Use: While it can promote trust and authenticity (e.g., on LinkedIn), using real names online can lead to:

- Harassment
- Stalking
- Impersonation

Pseudonymity/Anonymity:

- Platforms like Reddit or forums allow anonymous participation, protecting users’ real-life identities.
- However, anonymity can also encourage harmful behavior like trolling, hate speech, or illegal activities, making moderation harder.

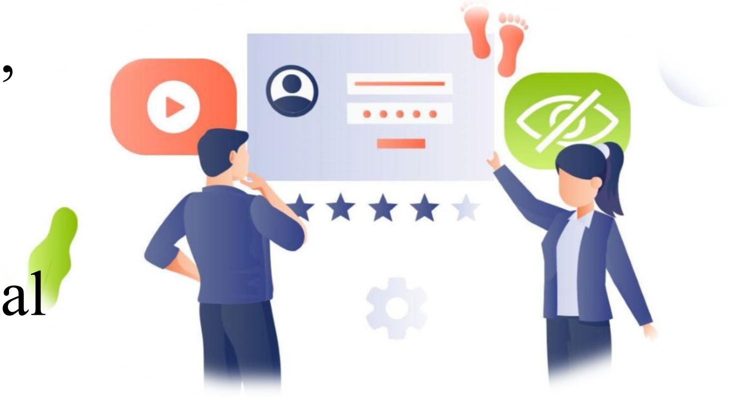
Balance Needed: Systems must find a way to balance free speech and personal safety with accountability.

🧾 Digital Footprint

Invisible Tracking: Users are often unaware that**:**

- Every website visited
- Every ad clicked
- Every product viewed or purchased is logged and analyzed.

Behavioral Profiling: Advertisers and data brokers use this information to build precise user profiles (interests, income, habits).



Consequences:

Systems must find a way to balance free speech and personal safety with accountability.

- **Price discrimination** (e.g., showing different prices based on browsing history)
- **Micro-targeted ads** that influence behavior and even voting choices
- **Employment/recruitment impact** based on online reputation

👁 Surveillance Concerns

Government Surveillance:

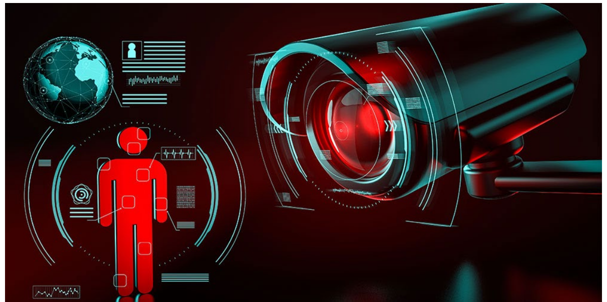
- National security agencies may monitor communication under the guise of protecting against terrorism or crime.
- E.g., PRISM program by NSA (Edward Snowden leaks).

Mass Surveillance:

- Raises ethical questions: When does surveillance cross into violating civil liberties?
- Minority communities may be disproportionately monitored.

Chilling Effect:

- Knowledge of surveillance may cause people to self-censor, limiting freedom of expression.



🛡 Cyberbullying and Doxxing

Cyberbullying:

- Online harassment can range from insults to threats.
- It often targets vulnerable groups: teens, minorities, LGBTQ+ individuals.
- Emotional consequences include depression, anxiety, and social withdrawal.

Doxxing:

- The act of publishing private/personal data (like phone numbers, addresses, school/work details) online without consent.
- Can lead to real-world dangers: stalking, threats, identity theft, job loss.

Legal & Ethical Concerns:

- Many countries now consider doxxing and cyberbullying as criminal offenses.
- Platforms are under pressure to improve moderation tools and victim support.

💼 3. Professional/Organizational Privacy Issues

🔍 1. Employee Monitoring

Employers may monitor employees' emails to prevent data leakage or ensure productivity. Tools can automatically flag suspicious content.

Software can record what employees' type. While useful for security, it's highly invasive and may breach privacy.

Used in logistics and field jobs to track location of employees. Raises concerns about constant surveillance and work-life boundaries.

🔐 2. Client and Customer Data Handling

- Organizations collect, store, and process personal data (e.g., name, address, payment details).
- Proper encryption, secure databases, and access restrictions must be enforced.
- Breaches can lead to legal penalties and loss of reputation.

📌 Example: A hospital mishandling patient records can face lawsuits and license revocation.

🧑‍⚕️ 3. Confidentiality Obligations

- Healthcare: Patient health records must be private (HIPAA in the USA).
- Finance: Bank account data must be protected from fraud.
- Legal: Lawyers must protect client data from unauthorized access.

These fields involve fiduciary duties a legal obligation to act in someone else's best interest with trust.

🛡️ 4. Access Control & Role-Based Access

- Role-Based Access Control (RBAC) ensures only authorized personnel access specific data.
- Example: An HR officer can access employee records, but not financial reports.
- Minimizes risk of accidental or malicious misuse of data.

👁️‍🗨️ 5. Workplace Surveillance vs. Employee Rights

- Cameras, browsing history, and call logs may be monitored.
- Employee consent and legal compliance are critical.
- Ethical question: How much monitoring is too much?

⚖️ Balance: Monitor for legitimate reasons (security, compliance), but respect personal boundaries.

🧨 6. Insider Threats & Ethical Data Use

- Insiders (employees) can misuse access for personal gain or revenge.
- Ethical culture, regular audits, and data access logs can deter misuse.
- Training programs should raise awareness about data ethics.

⚖️ 4. Legal and Ethical Frameworks

📜 1. Data Protection Laws

✅ GDPR (General Data Protection Regulation – EU)

Key Principles:

- Lawful, fair, and transparent data processing.
- Data minimization and accuracy.
- Right to access, correct, and erase personal data.

Hefty penalties for violations (up to €20 million or 4% of global turnover).

✅ HIPAA (Health Insurance Portability and Accountability Act – USA)

- Protects medical records and personal health data.
- Requires encryption, secure storage, and audit trails.
- Applies to hospitals, insurance companies, and any healthcare provider.

✅ Sri Lanka’s PDPA (Personal Data Protection Act)

- Enacted in 2022, to be fully enforced by 2025.
- Inspired by GDPR.
- Key Provisions:
  - Requires organizations to appoint Data Protection Officers (DPOs).
  - Provides rights for individuals to access and correct their data.
  - Restricts cross-border data transfer.
  - Mandatory breach notification.

💻 2. Computer Misuse and Cybercrime Acts

Sri Lanka's Computer Crimes Act (No. 24 of 2007):

- Criminalizes unauthorized access, system interference, and data theft.
- Covers hacking, identity theft, phishing, and spreading malware.

🧑‍💼 3. Ethical Responsibilities of ICT Professionals

Professional codes (e.g., ACM, IEEE) guide ICT behavior:

✅ 4. Informed Consent and Transparency

📌 *Example: A website should ask for cookie consent and explain what data is being tracked.*

🔧 5. Technologies and Tools Affecting Privacy

🍪 Cookies and Tracking Technologies

- Cookies are small files stored on a user's device to remember preferences or track activity.
  - First-party cookies: Used by the website you're visiting.
  - Third-party cookies: Placed by advertisers or other parties to track behavior across websites.
- Other tracking methods:
  - Web beacons, browser fingerprinting, and pixel tracking.
- Privacy Risk: Users may be tracked without informed consent, leading to profiling and behavioral advertising.

🔐 Encryption and Anonymization Tools

- **Encryption**: Converts data into unreadable form using algorithms and keys (e.g., AES, RSA).
  - Used in messaging apps (e.g., WhatsApp, Signal), VPNs, and secure web browsing (HTTPS).
- **Anonymization**: Removes personally identifiable information (PII) from datasets.
  - Example: Health data shared for research with names/IDs removed.
- **Privacy Benefit:** Protects data during storage and transmission.

🧠 Note: Weak or outdated encryption (e.g., MD5) can be easily broken, risking privacy.

🧬 Biometrics and Facial Recognition

- **Biometric authentication:** Uses fingerprints, iris scans, or facial features to identify individuals.
- **Facial recognition** is used in airports, phones, surveillance cameras.
- **Risks**:
  - **Mass surveillance** by governments or corporations.
  - **False positives** or racial bias in recognition systems.
  - **Biometric data theft** is irreversible – you can't change your face or fingerprint.

☁️ Cloud Computing and Data Storage Risks

- Cloud services (e.g., Google Drive, AWS, Microsoft Azure) store data offsite.
- **Benefits**: Scalability, access anywhere, collaboration.
- **Risks**:
  - Data stored in foreign jurisdictions may not be protected by local laws.
  - Data breaches if cloud security is weak or misconfigured.
  - Vendor lock-in: Dependency on the service provider.

🔐 Use of **end-to-end encryption** and **access control policies** is vital.

🌐 IoT (Internet of Things) Privacy Risks

- IoT includes smart devices like:
  - Smart TVs, fitness trackers, smart thermostats, connected cars.
- Many IoT devices:
  - Continuously collect user data (location, behavior, health).
  - Transmit data to cloud servers, often without strong encryption.
- Privacy Issues:
  - Lack of user awareness or control.
  - Data may be sold or exposed in a breach.
  - Insecure devices can be hacked and used as surveillance tools.

🧩 6. Privacy Threats and Violations

🎣 Phishing, Identity Theft, and Data Breaches

- **Phishing**: Deceptive emails or messages trick users into revealing personal info (e.g., bank logins).
- **Identity Theft:** Stolen PII (e.g., SSN, national ID) used to commit fraud.
- **Data Breaches:** Unauthorized access to databases (e.g., Facebook, Yahoo, Equifax incidents).
    - Often caused by poor security, insider threats, or unpatched vulnerabilities.
- 📌 Consequences:
    - Financial loss
    - Reputation damage
    - Legal action against the breached organization

📤 Third-Party Data Sharing and Behavioral Advertising

- Many websites and apps share user data with:
  - Advertisers
  - Analytics companies
  - Government or law enforcement (sometimes without user consent)
- **Behavioral Advertising**: Targets users based on their online activity (likes, searches, clicks).
- Users often lack transparency or control over how their data is used.

⚖️ Violates principles of informed consent and data minimization.

📱 Unauthorized Data Collection by Apps

- Some apps:
  - Request unnecessary permissions (e.g., a flashlight app asking for location access).
  - Collect and transmit user data without proper disclosure.
- **Risks**:
  - Children’s data being harvested.
  - Sensitive health or financial information being sold to third parties.

🔍 Example: Apps using **"permissions creep"** to gather more data than required for core functionality.

🎭 Deepfake and AI Misuse

- **Deepfakes**: Synthetic media generated using AI to mimic real people’s faces, voices, or actions.
- Can be used for:
  - Fake news
  - Political manipulation
  - Non-consensual adult content
- **AI Misuse**:
  - AI models trained on private or copyrighted data.
  - Surveillance systems using AI to monitor and profile individuals.
  - Bias in AI algorithms causing discriminatory outcomes.

🚨 Ethical and legal frameworks are still catching up with these rapidly advancing technologies.

🛡️ 7. Privacy Protection Measures

📉 1. Data Minimization and User Control

🔍 Data Minimization

- **Definition**: Only collect the data that is absolutely necessary for a specific purpose.
- **Why it's important**:
    - Reduces the risk of data breaches.
    - Complies with regulations (e.g., GDPR, PDPA).
- **Examples**:
    - A newsletter form asking only for an email address (not name, gender, etc.).
    - Limiting storage of customer credit card data after a transaction.

🎛️ User Control

- Users should have:
  - **Access** to their own data.
  - The ability to **edit or delete** it.
  - Control over **who** can see or share their data.
- **Tools**:
  - Privacy dashboards (like Google or Facebook).
  - Consent forms with clear opt-in/out options.

📌 Quote from GDPR: “Users should have control over their personal data.”

🧱 2. Privacy by Design and by Default

🔧 Privacy by Design (PbD)

- A proactive approach to privacy.
- Embed privacy into the design and architecture of IT systems and business processes from the start, not as an afterthought.
- Seven foundational principles (by Dr. Ann Cavoukian):
  - Proactive not reactive.
  - Privacy as the default setting.
  - Privacy embedded into design.
  - Full functionality (no trade-off).
  - End-to-end security.
  - Visibility and transparency.
  - User-centricity.

⚙️ **Privacy by Default**

- Systems must automatically provide privacy protections.
- Example:
  - Social media accounts set to "private" by default.
  - Apps not accessing location unless the user permits it.

🧠 Benefit: Users don’t have to actively protect their privacy—it’s built in.

📚 3. User Education and Awareness

🧠 Why it's important:

- Many privacy breaches happen due to user ignorance or negligence.
- Education empowers users to make informed decisions.

🔑 Key education topics:

- Recognizing phishing scams and fake websites.
- Understanding app permissions and data policies.
- Using strong passwords and enabling 2FA.
- Clearing browser history, cookies, and cache.

📢 How to deliver:

- Workshops in schools and workplaces.
- Awareness campaigns (e.g., Data Privacy Day – Jan 28).
- In-app privacy tips or tutorials.

📌 *"The weakest link in cybersecurity is often the human." – Common saying in IT security.*

🔐 4. Security Practices

🧱 Firewalls

- Hardware or software systems that **monitor and filter** incoming/outgoing traffic.
- Protect against unauthorized access to a network.

🦠 Antivirus and Anti-Malware

- Detect and remove malicious software (e.g., viruses, ransomware, spyware).
- Regular updates are essential for protection against new threats..

🌐 VPNs (Virtual Private Networks)

- Encrypt internet connections and mask the user’s IP address.
- Secure browsing, especially on public Wi-Fi.

🔑 Two-Factor Authentication (2FA)

- Adds an extra layer of security beyond a password.
- Requires a second factor, such as:
  - A mobile-generated code.
  - Fingerprint or facial recognition.
- Greatly reduces risk of unauthorized access—even if passwords are leaked.

🔐 Multi-Factor Authentication (MFA)

- Multi-Factor Authentication (MFA) is a security method that requires users to present two or more independent credentials (factors) to verify their identity before gaining access to a system, application, or data.

✅ The Three Main Types of Authentication Factors:

Factor Type	Description	Examples
1. Knowledge	Something the user **knows**	Password, PIN, answer to a secret question
2. Possession	Something the user **has**	Smartphone, security token, smart card
3. Inherence	Something the user **is**	Fingerprint, facial recognition, retina scan

🔐 MFA = 2 or more of these combined

MFA: Password + Smart Card + Fingerprint

🛡️ **Examples of MFA in Use**

1. Online Banking

- Password (knowledge) + OTP sent to phone (possession)

2. Gmail or Outlook Login

- Password + Google Authenticator app code

3. Corporate VPN Access

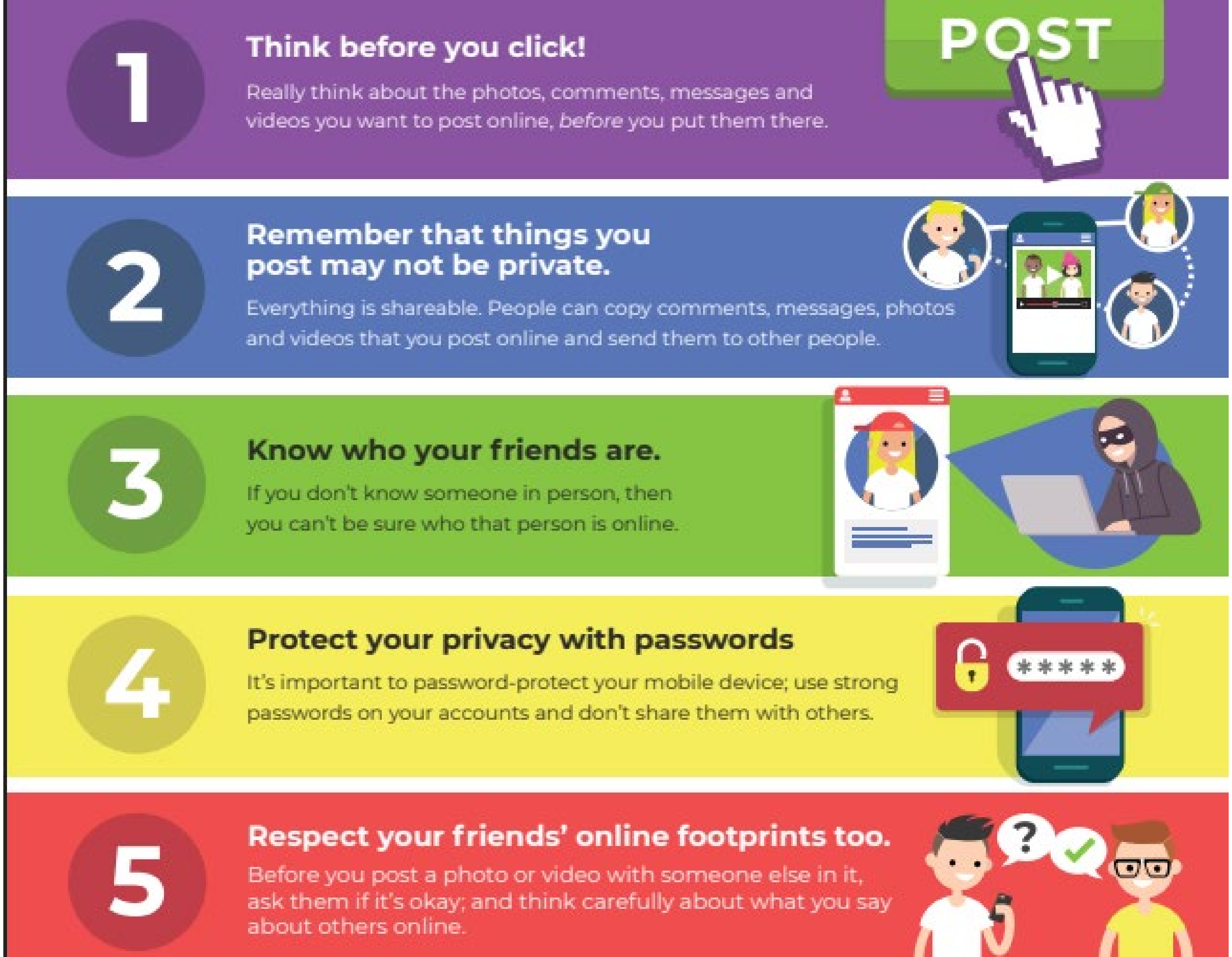
- Smart card (possession) + fingerprint (inherence)

4. University Systems

- Username/password + biometric scan or verification app (like Duo)

🔍 Other Recommended Practices:

- **Data encryption** (at rest and in transit).
- **Secure backups** and regular system updates.
- **Access control mechanisms** (e.g., Role-Based Access).
- **Audit trails** to detect unauthorized activity.



1 **Think before you click!**

Really think about the photos, comments, messages and videos you want to post online, *before* you put them there.

2 **Remember that things you post may not be private.**

Everything is shareable. People can copy comments, messages, photos and videos that you post online and send them to other people.

3 **Know who your friends are.**

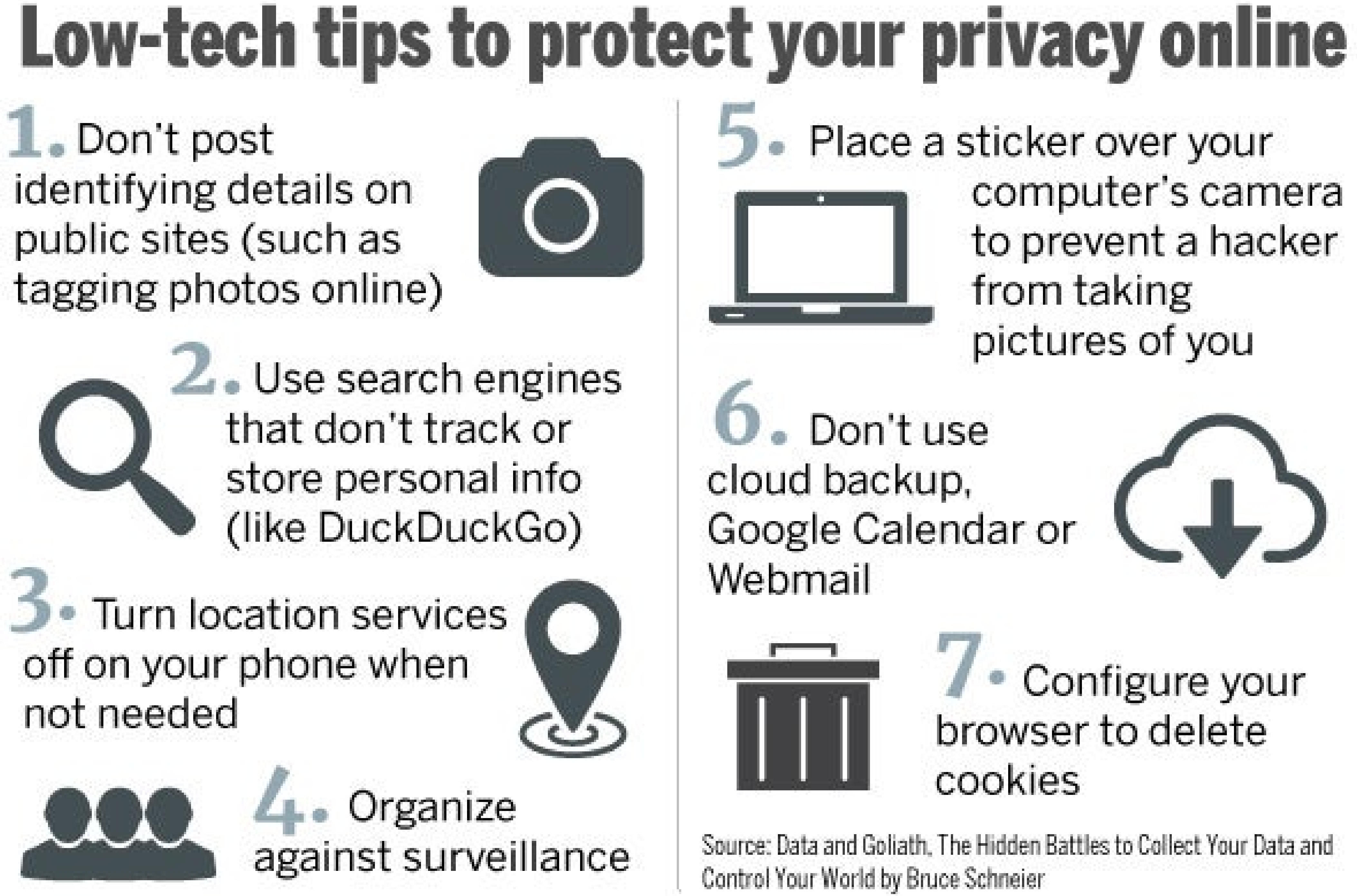
If you don't know someone in person, then you can't be sure who that person is online.

4 **Protect your privacy with passwords**

It's important to password-protect your mobile device; use strong passwords on your accounts and don't share them with others.

5 **Respect your friends' online footprints too.**

Before you post a photo or video with someone else in it, ask them if it's okay; and think carefully about what you say about others online.



Low-tech tips to protect your privacy online

1. Don't post identifying details on public sites (such as tagging photos online)

2. Use search engines that don't track or store personal info (like DuckDuckGo)

3. Turn location services off on your phone when not needed

4. Organize against surveillance

5. Place a sticker over your computer's camera to prevent a hacker from taking pictures of you

6. Don't use cloud backup, Google Calendar or Webmail

7. Configure your browser to delete cookies

Source: Data and Goliath, The Hidden Battles to Collect Your Data and Control Your World by Bruce Schneier

END