The media: internet and email

VOCABULARY PRACTICE

ADVANCED | C1

Name: _____ **Date:** _____

1 Match each advanced digital concept with its meaning.

1 end-to-end encryption	____	a preserving information for a defined period
2 transport encryption	____	b hidden image reporting that a message was opened
3 data retention	____	c protecting content so only endpoints can read it
4 traffic analysis	____	d protection applied while data travels between systems
5 link tracking	____	e inferring behaviour from communication patterns
6 pixel tracking	____	f privacy principle that information should follow contextual norms
7 consent fatigue	____	g repeated prompts weakening meaningful agreement
8 contextual integrity	____	h adding identifiers to URLs to monitor clicks

2 Complete the privacy and communication collocations.

consent | contextual | end-to-end | link | pixel | retention | traffic | transport

1 _____ encryption

2 _____ encryption

3 data _____ policy

4 _____ analysis

5 _____ tracking

6 _____ tracking

7 _____ fatigue

8 _____ integrity

3 Choose the concept that best explains the practice.

1 Only sender and recipient can read content: *end-to-end encryption / traffic analysis*.

2 A server connection is protected in transit: *transport encryption / contextual integrity*.

3 Messages are stored for seven years under *data retention / consent fatigue*.

4 Timing and recipient patterns reveal behaviour through *traffic analysis / link tracking*.

5 An identifier in a URL records clicks: *link tracking / pixel tracking*.

6 A hidden image reports email opening: *pixel tracking / transport encryption*.

7 Constant privacy prompts produce *consent fatigue / data retention*.

8 Using data outside expected norms violates *contextual integrity / end-to-end encryption*.

The media: internet and email

VOCABULARY PRACTICE

ADVANCED | C1

4 Complete the privacy audit with terms from the box.

consent fatigue | contextual integrity | data retention | end-to-end encryption | link tracking | pixel tracking | traffic analysis | transport encryption

The service advertises **1** _____, yet backups remain readable by the provider; its connection only guarantees **2** _____. A broad **3** _____ policy keeps message records indefinitely. Even without content, **4** _____ can infer who communicates when. Marketing URLs use **5** _____, while invisible images enable **6** _____. Repeated banners risk **7** _____. Overall, secondary use of contact data violates **8** _____ because it exceeds users' reasonable expectations.

5 Read the text and answer the questions concisely.

Private content, visible relations

Encryption can protect message content without hiding every fact about communication. Providers may still observe accounts, timing, frequency, device information and recipient patterns. This metadata can reveal relationships and routines even when the text remains unreadable. Privacy evaluation must therefore examine infrastructure, defaults, retention and secondary uses, not merely whether a lock icon appears. Meaningful consent also requires a realistic alternative to accepting surveillance.

1 What can encryption protect? _____

2 Does it hide every communication fact? _____

3 Name three facts providers may still observe. _____

4 What can metadata reveal? _____

5 Name three areas privacy evaluation should examine. _____

6 What does meaningful consent require? _____

6 Paraphrase using the expression in capitals.

1 Only the endpoints can read the content. **ENCRYPTED** ___

2 Patterns reveal relationships without message text. **TRAFFIC** _

3 The service keeps records indefinitely. **RETENTION** ___

4 Secondary use violates expected information norms. **INTEGRITY** _

OVER TO YOU

Write a **160-190 word** privacy audit of an email or online communication service. Distinguish content security from metadata privacy.

[ ] Use at least eight analytical terms. [ ] Examine defaults and retention. [ ] Assess whether consent is meaningful.

The media: internet and email

ANSWER KEY

1 Advanced digital concepts

1 **c** 2 **d** 3 **a** 4 **e** 5 **h** 6 **b** 7 **g** 8 **f**

2 Privacy collocations

1 **end-to-end** 2 **transport** 3 **retention** 4 **traffic** 5 **link** 6 **pixel** 7 **consent** 8 **contextual**

3 Conceptual distinctions

1 **end-to-end encryption** 2 **transport encryption** 3 **data retention** 4 **traffic analysis**
5 **link tracking** 6 **pixel tracking** 7 **consent fatigue** 8 **contextual integrity**

4 Privacy audit

1 **end-to-end encryption** 2 **transport encryption** 3 **data retention** 4 **traffic analysis**
5 **link tracking** 6 **pixel tracking** 7 **consent fatigue** 8 **contextual integrity**

5 Reading - suggested answers

1 Message content. 2 No. 3 Any three: accounts, timing, frequency, devices, recipients. 4 Relationships and routines.
5 Any three: infrastructure, defaults, retention, secondary uses. 6 A realistic alternative to surveillance.

6 Paraphrasing - possible answers

1 The content is **end-to-end encrypted**. 2 **Traffic analysis** reveals relationships. 3 The service has indefinite data **retention**.
4 The use violates contextual **integrity**.

Over to you: Answers will vary. Check security distinctions, metadata risks and consent.