**Review Questions FOR CHAPTER 3**

You can find the answers in Appendix A.

**1.** All of these are methods of data discovery, except:

**A.** Content-based

**B.** User-based

**C.** Label-based

**D.** Metadata-based

**2.** Data labels could include all the following, except:

**A.** Date data was created

**B.** Data owner

**C.** Data value

**D.** Data of scheduled destruction

**3.** Data labels could include all the following, except:

**A.** Source

**B.** Delivery vendor

**C.** Handling restrictions

**D.** Jurisdiction

**4.** Data labels could include all the following, except:

**A.** Confidentiality level

**B.** Distribution limitations

**C.** Access restrictions

**D.** Multifactor authentication

**5.** All the following are data analytics modes, except:

**A.** Real-time analytics

**B.** Datamining

**C.** Agile business intelligence

**D.** Refractory iterations

**6.** In the cloud motif, the data owner is usually:

**A.** In another jurisdiction

**B.** The cloud customer

**C.** The cloud provider

**D.** The cloud access security broker

**7.** In the cloud motif, the data processor is usually:

**A.** The party that assigns access rights

**B.** The cloud customer

**C.** The cloud provider

**D.** The cloud access security broker

**8.** Every security program and process should have which of the following?

**A.** Foundational policy

**B.** Severe penalties

**C.** Multifactor authentication

**D.** Homomorphic encryption

**9.** All policies within the organization should include a section that includes all of the following, except:

**A.** Policy maintenance

**B.** Policy review

**C.** Policy enforcement

**D.** Policy adjudication

**10.** The most pragmatic option for data disposal in the cloud is which of the following?

**A.** Melting

**B.** Cryptoshredding

**C.** Cold fusion

**D.** Overwriting

**11.** What is the intellectual property protection for the tangible expression of a creative idea?

**A.** Copyright

**B.** Patent

**C.** Trademark

**D.** Trade secret

**12.** What is the intellectual property protection for a useful manufacturing innovation?

**A.** Copyright

**B.** Patent

**C.** Trademark

**D.** Trade secret

**13.** What is the intellectual property protection for a very valuable set of sales leads?

**A.** Copyright

**B.** Patent

**C.** Trademark

**D.** Trade secret

**14.** What is the intellectual property protection for a confidential recipe for muffins?

**A.** Copyright

**B.** Patent

**C.** Trademark

**D.** Trade secret

**15.** What is the intellectual property protection for the logo of a new video game?

**A.** Copyright

**B.** Patent

**C.** Trademark

**D.** Trade secret

**16.** What is the aspect of the DMCA that has often been abused and places the burden of proof on the accused?

**A.** Online service provider exemption

**B.** Decryption program prohibition

**C.** Takedown notice

**D.** Puppet plasticity

**17.** What is the federal agency that accepts applications for new patents?

**A.** USDA

**B.** USPTO

**C.** OSHA

**D.** SEC

**18.** DRM tools use a variety of methods for enforcement of intellectual property rights. These include all the following, except:

**A.** Support-based licensing

**B.** Local agent enforcement

**C.** Dip switch validity

**D.** Media-present checks

**19.** All of the following regions have at least one country with an overarching, federal privacy

law protecting personal data of its citizens, except:

**A.** Asia

**B.** Europe

**C.** South America

**D.** The United States

**20.** DRM solutions should generally include all the following functions, except:

**A.** Persistency

**B.** Automatic self-destruct

**C.** Automatic expiration

**D.** Dynamic policy control

**Chapter 3: Data Classification**

**1.** B. All the others are valid methods of data discovery; user-based is a red herring with no

meaning.

**2.** C. All the others might be included in data labels, but we don’t usually include data value,

since it is prone to change frequently, and because it might not be information we want to

disclose to anyone who does not have need to know.

**3.** B. All the others might be included in data labels, but we don’t include delivery vendor,

which is nonsense in context.

Chapter 3: Data Classification **313**

**4.** D. All the others might be included in data labels, but multifactor authentication is a procedure

used for access control, not a label.

**5.** D. All the others are data analytics methods, but “refractory iterations” is a nonsense term

thrown in as a red herring.

**6.** B. The data owner is usually considered the cloud customer in a cloud configuration; the

data in question is the customer’s information, being processed in the cloud. The cloud provider

is only leasing services and hardware to the customer. The cloud access security broker

(CASB) only handles access control on behalf of the cloud customer, and is not in direct

contact with the production data.

**7.** C. In legal terms, when “data processor” is defined, it refers to anyone who stores, handles,

moves, or manipulates data on behalf of the data owner or controller. In the cloud computing

realm, this is the cloud provider.

**8.** A. Policy drives all programs and functions in the organization; the organization should

not conduct any operations that don’t have a policy governing them. Penalties may or may

not be an element of policy, and severity depends on the topic. Multifactor authentication

and homomorphic encryption are red herrings here.

**9.** D. All the elements except adjudication need to be addressed in each policy. Adjudication is

not an element of policy.

**10.** B We don’t have physical ownership, control, or even access to the devices holding the data,

so physical destruction, including melting, is not an option. Overwriting is a possibility,

but it is complicated by the difficulty of locating all the sectors and storage areas that might

have contained our data, and by the likelihood that constant backups in the cloud increase

the chance we’ll miss something as it’s being overwritten. Cryptoshredding is the only reasonable

alternative. Cold fusion is a red herring.

**11.** A. Copyrights are protected tangible expressions of creative works. The other answers

listed are answers to subsequent questions.

**12.** B. Patents protect processes (as well as inventions, new plantlife, and decorative patterns).

The other answers listed are answers to other questions.

**13.** D. Confidential sales and marketing materials unique to the organization are trade secrets.

The other answers listed are answers to other questions.

**14.** D. Confidential recipes unique to the organization are trade secrets. The other answers

listed are answers to other questions.

**15.** C. Logos and symbols and phrases and color schemes that describe brands are trademarks.

The other answers listed are answers to other questions.

**16.** C. The DMCA provision for takedown notices allows copyright holders to demand

removal of suspect content from the web, and puts the burden of proof on whoever posted

the material; this function has been abused by griefers and trolls and overzealous content

producers. The OSP exemption providers a safe harbor provision for web hosts.

**314** Appendix A ■ Answers to the Review Questions

The decryption program prohibition makes DeCSS and other similar programs illegal.

Puppet plasticity is a nonsense term used for a red herring.

**17.** B. The U.S. Patent and Trademark Office accepts, reviews, and approves applications for

new patents. The USDA creates and enforces agriculture regulation. OSHA oversees workplace

safety regulations. The SEC regulates publicly traded corporations.

**18.** C. DRM solutions use all these methods except for dip switch validity, which is a nonsense

term.

**19.** D. The United States does not have a single, overarching personal privacy law; instead,

the U.S. often protects PII by industry (HIPAA, GLBA, FERPA, and so forth.). All EU

member countries adhere to the Data Protection Regulation. Argentina’s Personal Data

Protection Act cleaves to the EU Regulation, as does Japan’s Act on the Protection of

Personal Information.

**20.** B. DRM tools should include all the functions listed except for self-destruction, which

might hurt someone.