Consumers should look for some of the following terms when reading EULAs or terms of service contracts:

- **Use**—Does the contract give the vendor the right to change the service or product whenever it wants? Does the vendor have the unilateral right to stop providing certain important features? Does the vendor have the right to investigate how the user uses the product or service to determine if there has been a violation of the contract?
- **Fees**—Does the contract have any hidden licensing fees or any hidden upgrade, support, or maintenance fees?
- **Representations and warranties**—Does acceptance of the contract mean that the consumer bears all economic risk related to downloading and using the product or service? What's the consumer's recourse if the product or service includes viruses and errors, or causes data loss or hardware/software failure? Does the contract state that use of the product or service is at the consumer's own risk? Does it state that the products are provided "as is?"
- **Advertising**—Does the contract give the vendor the right to include embedded software or spyware with the desired product or service? Does acceptance of the contract mean that the consumer consents to receiving advertising content, from either the vendor or other third parties? Is the vendor allowed to collect usage data and other statistics related to the consumer's use of the service? How is this data used?
- **Criticism**—Does the contract specifically prohibit the consumer from publicly criticizing the product or service?
- **Updates**—Does the contract state that updates are covered by the original contract? Are updates covered by a new contract that the consumer must specifically agree to?
- **Termination and breach**—Does the contract allow a consumer to stop using the product or service at any time? Can the consumer stop using the product by uninstalling and destroying software and documentation? Must the vendor destroy any consumer personal data it has collected when the contract ends?
- **Boilerplate terms**—Does the contract state that it's subject to change without notice? Does it state that the consumer specifically consents to any modifications of the contract without notice? Does it include dispute resolution terms? Does it contain jurisdiction language? Does it require that consumers file lawsuits in a certain state and county within that state?

> **NOTE**
>
> A consumer should exercise caution if a contract says that products or services are provided "as is" or use is at the consumers' "own risk." This means that the seller is disclaiming a number of different consumer protection warranties.

> **NOTE**
>
> Terms in a contract that state that consumers must file lawsuits in a certain state or county in that state are called forum selection clauses. Contracting parties use forum selection clauses to control questions about jurisdiction. They also use them so that they can litigate lawsuits in front of a familiar court. It's the legal equivalent of "home court advantage."

Consumers must think about what they're willing to agree to in order to use a particular product or online service. They must balance their need for the use of a product or service with other contract terms that might place them, or their data, at a disadvantage.

Emerging Contract Law Issues

New developments in Internet-based products and services are causing people and organizations to think more about information security. People and entities must take steps to protect and secure information at the same time as information is being shared more than ever before. Entities use contracts to make sure that their own data, and the personal information of their customers, is protected when it's shared.

Sometimes the law requires a contract. For example, both the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) require covered businesses to enter into contracts with their third-party service providers to protect data. These contracts hold the third parties accountable for the minimum levels of data privacy and information security protection that those laws require for certain types of information.

> **NOTE**
> A third-party agreement under HIPAA is called a business associate's agreement.

Entities also enter into these contracts voluntarily when they use new services or buy new products. The importance of including data security terms in these contracts continues to grow. The newest development in Internet-based products and services that highlights information security issues is cloud computing.

Cloud Computing

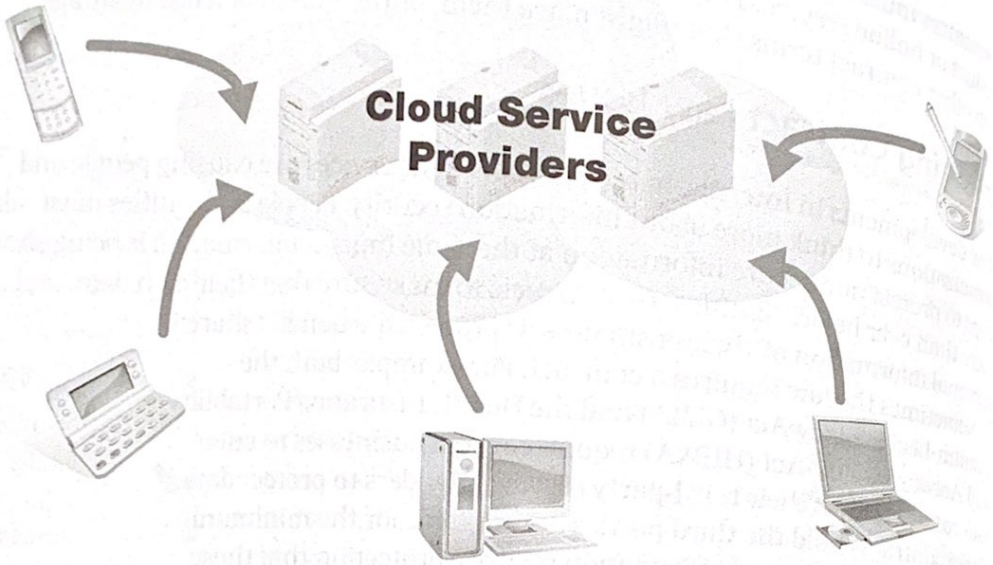
The definition and limits of cloud computing are still evolving. **Cloud computing** is a type of computing where both applications and infrastructure capabilities can be provided to end users through the Internet. Through cloud computing, entities no longer have to own their own computer hardware and infrastructure. They can purchase these services from cloud service providers. They only pay for the infrastructure and applications that they need. Figure 11-1 is a basic cloud computing diagram.

Cloud computing is not just for businesses. Individuals also use cloud computing services. Yahoo! Mail is a cloud service. Google's Picasa photo-sharing service is a cloud service. So is Mozy's online computer backup service.

> **NOTE**
> SaaS refers to the purchase of application services over the Internet. Cloud computing refers to the purchase of application, infrastructure, and storage capabilities through the Internet.

Cloud computing has its beginnings in the **Software as a Service (SaaS)** model. In the SaaS model, a vendor hosts a Web-based application and provides that application to its customers. The customers purchase access to hosted application. The entities access these services over the Internet. The SaaS vendor hosts the applications and maintains the infrastructure necessary for running the application.

FIGURE 11-1
Basic cloud computing diagram.



> **NOTE**
> Gartner, Inc., is a respected company that provides internet technology advice and research. You can learn more about Gartner, Inc., at *http://www.gartner.com/technology/about.jsp*.

> **NOTE**
> In 2007, Dell, Inc. tried to trademark the term "cloud computing." The U.S. Patent and Trademark Office rejected the trademark because it was too generic and described services offered by many companies.

Cloud computing consumers can purchase infrastructure services such as data storage, backup facilities, and data processing. Cloud computing also includes the purchase of applications traditionally provided under the SaaS model such as e-mail services. Cloud computing is attractive to many entities. Gartner, Inc., estimates that companies will spend $677 billion on cloud services through 2016.[30]

Many organizations believe that using cloud computing will help them save money on information technology (IT) costs. Cost savings include not spending money upfront on data centers, electricity, equipment, and physical security. It also might help save money on IT staff. Cloud computing is seen as scalable with the organization's own growth. An organization purchases only the services it needs at a fixed point in time. It can always buy more cloud services when it needs them. Buying cloud services can be faster than building the organization's own IT infrastructure.

Cloud computing leads to situations where an entity's data isn't stored on its own physical computing infrastructure. This makes information security practitioners (and lawyers) nervous. A survey in late 2012 showed that information security topped a list of U.S. government technology professionals' concerns about cloud computing.[31] Information security concerns about cloud computing include:

FYI

A U.S. Department of Justice bulletin issued in 2009 showed that state-court contract law cases took almost two years to resolve. This statistic was for 2005, the latest year for which data is available at this writing. You can read the report at *http://bjs.ojp.usdoj.gov/content/pub/pdf/cbajtsc05.pdf*.

- Loss of control of data, leading to a loss of security or lessened security
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers
- Dependency on a third party for critical infrastructure and data-handling processes
- Potential security and technological defects in the cloud provider's infrastructure
- No control over the third parties that a cloud vendor might contract with
- Loss of an entity's own competence in managing IT infrastructure security

There also are legal concerns about cloud computing. Contract law governs a cloud computing relationship. Disputes over the terms of the contract could be costly to resolve. They also could take too long to resolve. A lengthy dispute about critical services could harm a business and affect its ability to operate.

Another legal concern about cloud computing is where data and infrastructure are located. Local law might control how entities handle data. Questions of who owns the data also could be influenced by the law of the state where data is located, assuming that the data is actually stored in the United States. Location of the data could have impact on how that data is provided in response to a public records request, subpoena, or court order. There also could be different rules for how that data must be secured. It also could affect how companies should respond to a breach of the systems used to store their data.

Information Security Terms in Contracts

Entities entering into contracts for cloud computing services need to consider a number of items from a law and information security standpoint. A cloud computing consumer will want to make sure that a cloud computing provider physically protects the cloud computing infrastructure that holds the consumer's data. A cloud computing consumer also will want to make sure that the cloud computing provider follows good information security practices and protects the security of any data on that infrastructure.

NOTE

Since the cloud computing relationships include data, this is one time where an entity will want to make sure that it has a formal written contract with its vendors.

There are a number of information security issues to consider in any cloud computing contract. These same themes also can be considered in any contract where an entity's data might be stored, processed, transmitted, or handled by another party.

It's important for both contracting parties to understand the scope of data that they must protect in a contract. The parties must think about the following:

- How data is defined
- How data is used
- How data is protected
- How the parties meet their legal and regulatory requirements

Data Definition and Use

> **NOTE**
> A contract should define the data elements used by the parties. For instance, if personal information is transmitted between the parties, then the contract should specify what data elements are considered personal information. This definition could change depending upon the type of data transmitted between the parties.

Both parties to a contract must understand the type of data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the data owned by each party. The parties also must clearly define data that must be protected.

It's also important for the parties to clearly specify in the contract how they can use any data that they share. An entity will want to make sure that its vendor, or cloud computing provider, doesn't use its data in a way that would violate its privacy policies. An entity also will want to make sure that there are limits on the vendors own use of the data. For instance, a vendor shouldn't be able to share the entity's data with other third parties without their permission. Finally, the contract should specify what happens to the data when the contract ends.

Data use terms also should specify what the parties can't do with certain types of data. For example, if credit card information is transmitted as part of a cloud computing contract, that contract should require the vendor to comply with the Payment Card Industry Data Security Standards.

General Data Protection Terms

> **NOTE**
> A minimum level of acceptable information security is called a baseline.

An entity may want to specify particular data protection terms in a contract. These terms are more specific than data use terms. For instance, an entity may want to include terms that state the specific administrative, technical, and physical safeguards that a vendor must use. When an entity includes these types of terms, they are trying to guarantee a minimum level of confidentiality, integrity, and availability.

An entity could include the following contract terms to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms

- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

Contracting parties can use resources developed by the National Institute of Standards and Technology (NIST) to make sure that a contract includes the appropriate controls. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) also have prepared information security controls guidance.

Compliance with Legal and Regulatory Requirements

Sometimes laws or regulatory controls will influence the relationship covered by a contract. This happens when the data or processes used between the parties falls within the scope of a particular law. GLBA and HIPAA were already mentioned as two federal laws that pull certain types of data and relationships into their scope.

State laws also could be implicated. For example, Massachusetts[32] and Nevada[33] have laws that require the personal information of state residents to be encrypted in certain instances. This requirement would need to be specified in a contract in order to ensure that a vendor meets it.

> **NOTE**
>
> Contracts also have to include terms that help entities meet their breach notification duties in the event that a vendor's systems are compromised and the entity's data is disclosed.

Additional terms that a contract should have to address regulatory requirements include:

- GLBA language if financial data is used or transmitted between the parties
- HIPAA language if health information is used or transmitted between the parties
- Family Educational Rights and Privacy Act (FERPA) of 1974 language if student information is used or transmitted between the parties
- Language protecting the intellectual property rights of each party

An entity also will want to make sure that a contract contains terms that require the vendor to cooperate with security incident investigations. This is so the entity can meet its regulatory requirements. A contract also must have terms that require each party to assist the other with third party litigation that occurs because of the contractual relationship. For example, a contract should state that the vendor will assist the entity with any litigation against the entity that arises because of a breach of the security of the vendor's systems.

As new technologies emerge and are developed, the rules for using that technology will become very important. One way that entities can establish rules is through contractual agreements.

Case Studies and Examples

The following case studies and examples show how the concepts discussed in this chapter are used. These case studies are real-world examples of contract law issues.

Contract Formation via E-mail

Parties continue to argue about the enforceability of electronic contracts. California adopted its version of the Uniform Electronic Transactions Act in 1999. This case began before California enacted its UETA law. Would the case have even reached a U.S. Court of Appeals if California's UETA law had been in existence when this transaction began?

Stewart Lamle invented a board game called Farook. He obtained two U.S. patents for his game. In May 1996, Lamle began negotiating with toy-giant Mattel to license his game. They signed a preliminary agreement for $25,000. Under this agreement, Lamle agreed not to license the game to anyone else until after June 15, 1997.

On June 11, 1997, the parties met and discussed the terms of a licensing agreement. They agreed to terms regarding the length of the license agreement. They also agreed to geographic scope of the agreement, the percentage of royalties, and a schedule for payment of royalties. Mattel asked Lamle to draft a formal contract. It promised it would sign an agreement before January 1, 1998.

On June 26, 1997, a Mattel employee sent Lamle an e-mail with the subject line "Farook Deal." The e-mail repeated the terms agreed to at the earlier meeting. It also stated specifically that Mattel agreed in principle to the agreement and was waiting for the contract. The e-mail concluded with a closing salutation and the employee's full name. Lamle faxed a draft licensing agreement to Mattel on August 19, 1997.

In August, Mattel displayed Farook at its Pre-Toy Fair. The purpose of the fair was to gauge potential interest in new toys. After the fair, Mattel decided that it wasn't interested in Farook. It notified Lamle in October.

Lamle sued for breach of contract in October 1999. He also made claims of patent infringement and intentional interference with economic relations.

> **NOTE**
>
> One of the most interesting things about this case is that Lamle represented himself *pro se*. *Pro se* means that a person isn't represented by a lawyer. Lamle represented himself throughout the whole case *pro se*. Lamle isn't a lawyer.

The District Court for the Central District of California granted summary judgment in favor of Mattel. Summary judgment means that a court has decided that there's not a factual dispute between the parties. Lamle appealed the grant of summary judgment. The Federal Circuit Court of Appeals upheld his appeal and sent the case back to District Court.

The District Court again granted summary judgment for Mattel. The District Court rejected Lamle's breach of contract claim. It held that no reasonable juror would believe that there was a contract between the parties. It also held that even if there was a contract, it wasn't enforceable because it wasn't in writing as required by California's Statute of Frauds. Lamle appealed again.

FYI

States have statute of limitations rules. This means that people must bring a lawsuit for injuries that they have incurred within a certain period of time. In California, lawsuits for breach of oral contracts must be filed within two years of the date of the breach. The statute of limitations for written contracts is four years. Lamle sued Mattel exactly two years from the date that Mattel notified him that it wasn't interested in Farook. Why did Lamle sue at the two-year mark?

The Federal Circuit Court of Appeals reviewed the conduct of the parties. It held that there was a genuine question whether the parties had reached mutual agreement on contractual terms at the June 11 meeting. It held that a trial was needed and evidence should be presented on the issue of mutual assent.

The court also discussed California's Statute of Frauds. It reviewed the June 26 e-mail from the Mattel employee. It held that the name of the Mattel employee at the end of the e-mail was enough to overcome the signed writing requirements of the Statute of Frauds. It said that its ruling was consistent with other California laws that state that a typewritten name is considered a signature.

The Court also noted that if the e-mail from the Mattel employee had been sent after January 1, 2000, there would be no question at all whether the e-mail constituted a signed writing for Statute of Frauds purposes. California's version of the UETA went into effect at that time.

The Federal Circuit Court of Appeals ruling gave Lamle the right to have a jury trial on his breach of contract claim. Lamle and Mattel eventually settled their claims against one another.

You can read the Court's opinion at *http://scholar.google.com/scholar_case?case=5607112815760928119*.

Contract Dispute Statistics

The U.S. Department of Justice (DOJ) compiles statistics on court cases in state courts. One of its series is "Civil Trial Cases and Verdicts in Large Counties." This series gives statistics on cases in a national sample of urban and rural jurisdictions. The DOJ began collecting and reviewing this data in 1992.

In 2009, the DOJ issued a special study on contract cases heard in state courts.[34] The study looked at only state-court contract cases. It didn't look at contract cases tried in federal court.

The study found that two-out-of-three plaintiffs won their contract trials. Plaintiffs were more likely to win cases that were decided by a judge instead of a jury. The study found that juries award higher damages than judges do.

Take some time to review the Contract Bench and Jury Trials in State Courts (2005) report. What statistics surprised you?

NOTE

All of the studies in the "Civil Trial Cases and Verdicts in Large Counties" series can be read at *http://www.bjs.gov/index.cfm?ty=pbse&sid=15*.