Solution and Answer Guide

Miller, Business Law Today, Comprehensive Edition: Text & Cases 13e, 9780357634783;   
Chapter 08: Internet Law, Social Media, and Privacy

Table of Contents

[Critical Thinking Questions in Features 1](#_Toc62740195)

[Adapting the Law to the Online Environment 1](#_Toc62740196)

[Critical Thinking Questions in Cases 1](#_Toc62740197)

[Case 4.1 1](#_Toc62740198)

[Case 4.2 2](#_Toc62740199)

[Case 4.3 2](#_Toc62740200)

[Chapter Review 3](#_Toc62740201)

[Practice and Review 3](#_Toc62740202)

[Practice and Review: Debate This 4](#_Toc62740203)

[Issue Spotters 5](#_Toc62740204)

[Business Scenarios and Case Problems 5](#_Toc62740205)

[Critical Thinking and Writing Assignments 13](#_Toc62740206)

# Critical Thinking Questions in Features

Adapting the Law to the Online Environment

1. If LoL is free to players, why would a Chinese company want to copy it?

Solution

There is usually a charge to download any app. Therefore, copying an extremely popular multiplayer online game can yield a sizable revenue stream from those who download the app. Additionally, anything on the Internet is open to advertising. Advertising leads to revenue streams.

# Critical Thinking Questions in Cases

Case 8.1

1. Suppose that the candyland.com website had not been sexually explicit but had sold candy. Would the result have been the same? Explain.

Solution

Probably. In this circumstance, Hasbro could most likely demonstrate a likelihood of prevailing on a claim that the defendant violated the applicable federal and state statutes against trademark dilution. The Hasbro trademark is famous, the defendant would presumably be using it without permission, and that use would arguably diminish the quality of the Hasbro mark.

1. How can companies protect themselves from situations such as the one described in this case? What limits each company’s ability to be fully protected?

Solution

To protect themselves from others who create websites that have similar domain names, companies can be vigilant and act quickly and forcefully to enforce their rights. A company’s ability to be fully protected is limited chiefly by its resources and by the skill of the persons on whom the company relies to protect it.

Case 8.2

1. Should an ISP be liable for copyright infringement by its subscribers regardless of whether the ISP is aware of the violation? Why or why not?

Solution

No, an ISP should not be liable for the infringement activities of its subscribers unless the ISP is aware of the violations. As under the DMCA, and in the *BMG* case, an ISP should be liable only if it is aware of the infringement and fails to take reasonably meaningful action to stop it, or at least to terminate the subscriber’s service.

The importance of intellectual property supports the protection of rights to its ownership. Prohibiting infringement is a significant component of this protection. Prosecuting violators is a material part of this prohibition.

But the subscribers to ISPs, like the users of other Internet services, can more easily take advantage of those services to engage in illicit conduct, such as copyright infringement, than the providers can quickly police. Those providers should be held liable for failing to discourage such behavior and for failing to act once they know of it. Until they are aware of it, however, it would be unfair to hold them to account.

1. Could Cox legitimately claim that it had no knowledge of subscribers who infringed BMG’s copyrights, since the ISP was deleting all of BMG’s infringement notices? Explain.

Solution

No, Cox could not legitimately claim that by deleting all of BMG’s infringement notices, it was unaware of the activity of those among its subscribers who infringed the sender’s copyrights. In fact, the decision to delete all such notices would undercut any contention that it was unaware of any infringement by any subscriber.

Of course, in the *BMG* case, the court reasoned that when Cox decided to delete all infringement notices received from BMG, the ISP dispensed with terminating subscribers who repeatedly infringed BMG’s copyrights. This was in addition to the ISP’s general unstated policy to terminate no subscribers for infringement, contrary to its own stated policy. In effect, Cox had no infringement policy.

Case 8.3

1. Is a violation of an individual’s right to privacy, without more, enough to sustain a legal cause, or should additional consequences be required to maintain an action? Explain.

Solution

Yes, an intrusion into an individual’s privacy is sufficient to sustain a legal cause of action. It constitutes a sufficiently concrete injury to support the cause. Additional consequences are not necessary.

Violations of the right to privacy have long been subject to actions at common law. Historically recognized as an “unreasonable intrusion upon the seclusion of another,” the cause has traditionally been extended to incorporate, among other things, “tapping” landline phone wires and opening others’ mail. Referred to as the invasion of a “substantive right,” the intrusion itself is enough to impose liability.

The Electronic Communications Privacy Act (ECPA), which was the basis for the plaintiffs’ claim in the *Campbell* case, codifies privacy torts into a federal statute making the intentional interception of any “electronic communication” a ground for an action. Additional consequences are not required. At common law or under the ECPA, a plaintiff does need not to allege or show any further harm to succeed.

1. Should Facebook pay the platform’s users for Facebook’s use of their private data? Discuss.

Solution

Yes, Facebook should pay its users for the use of their private data, particularly when those uses include the facilitation of targeted advertising. Users should be viewed as the owner of their data, and Facebook, which is profiting from its use, should be required to pay for it.

Further, individuals should have control over their data. They should be asked whether they want their data used, whom they would permit to use it, and the uses to which it would be applied. As with any property, the owners should be able to sell or not sell it as they choose.

Conversely, no, Facebook does not need to pay its users for the use of their data. Layers of complexity challenge the categorization of data, such as that collected and used by Facebook, as property subject to the traditional definition of ownership. Its marketability by individual “owners” is doubtful—it is hard for individuals to trade. If it cannot be easily sold, its ownership is arguably incomplete.

# Chapter Review

Practice and Review

While he was in high school, Joel Gibb downloaded numerous songs to his smartphone from an unlicensed file-sharing service. He used portions of the copyrighted songs when he recorded his own band and posted videos on YouTube and Facebook. He also used BitTorrent to download several movies from the Internet. Now Gibb has applied to Boston University. The admissions office has requested access to his Facebook password, and he has complied. Using the information presented in the chapter, answer the following questions.

1. What laws, if any, did Gibb violate by downloading music and videos from the Internet?

Solution

Technology has vastly increased the potential for copyright infringement. Generally, whenever a party downloads music into a computer’s random access memory, or RAM, without authorization, a copyright is infringed. Thus, when file-sharing is used to download others’ stored music files, copyright issues arise. Recording artists and their labels stand to lose large amounts of royalties and revenues if relatively few digital downloads or CDs are purchased and then made available on distributed networks.

1. Was Gibb’s use of portions of copyrighted songs in his own music illegal? Explain.

Solution

At least one federal court has held that sampling a copyrighted sound recording of any length constitutes copyright infringement. Some other federal courts have not found that digital sampling is always illegal. Some courts have allowed the defense of fair use, while others have not.

1. Can individuals legally post copyrighted content on their Facebook pages? Why or why not?

Solution

Piracy of copyrighted materials online can occur even if posting the materials is “altruistic” in nature—unauthorized copies are posted simply to be shared with others. The law extends criminal liability for the piracy of copyrighted materials to persons who exchange unauthorized copies of copyrighted works without realizing a profit.

1. Did Boston University violate any laws when it asked Joel to provide his Facebook password? Explain.

Solution

Many states have enacted legislation to protect individuals from having to disclose their social media passwords. The federal government is also considering legislation that would prohibit employers and schools from demanding passwords to social media accounts. If, at the time of the application, however, Massachusetts was not covered by any of these statutes, Boston University would not have violated any law by asking for Gibbs’s password, which he then voluntarily divulged.

Practice and Review: Debate This

1. Internet service providers should be subject to the same defamation laws as newspapers, magazines, and television and radio stations.

Solution

Those who support this position argue that it is not fair to those who are defamed by others on the Internet to not have recourse against the ISP. After all, there should be no difference between traditional media outlets and the Internet. Those who are against applying similar defamation law to all media argue that ISPs cannot become censors. They point out the technological inability of ISPs to monitor all of the statements that go through their servers.

Issue Spotters

1. Karl self-publishes a cookbook titled *Hole Foods*, in which he sets out recipes for donuts, Bundt cakes, tortellini, and other foods with holes. To publicize the book, Karl designs the website *holefoods.com*. Karl appropriates the key words of other cooking and cookbook sites with more frequent hits so *that holefoods.com will* appear in the same search engine results as the more popular sites. Has Karl done anything wrong? Explain.

Solution

Karl may have committed trademark infringement. Search engines compile their results by looking through websites’ key-word fields. A site that appropriates the key words of other sites with more frequent hits will appear in the same search engine results as the more popular sites. But using another’s trademark as a key word without the owner’s permission normally constitutes trademark infringement. Of course, some uses of another’s trademark as a meta tag may be permissible if the use is reasonably necessary and does not suggest that the owner authorized or sponsored the use.

1. Eagle Corporation began marketing software in 2010 under the mark “Eagle.” In 2019, Eagle.com, Inc., a differ­ent company selling different products, begins to use *eagle* as part of its URL and registers it as a domain name. Can Eagle Corporation stop this use of *eagle*? If so, what must the company show?

Solution

Yes. This may be an instance of trademark dilution. Dilution occurs when a trademark is used, without permission, in a way that diminishes the distinctive quality of the mark. Dilution does not require proof that consumers are likely to be confused by the use of the unauthorized mark. The products involved do not have to be similar. Dilution does require, however, that a mark be famous when the dilution occurs.

Business Scenarios and Case Problems

1. **Privacy.** See You, Inc., is an online social network. SeeYou’s members develop personalized profiles to share information— photos, videos, stories, activity updates, and other items—with other members. Members post the information that they want to share and decide with whom they want to share it. SeeYou launched a program to allow members to share with others what they do elsewhere online. For example, if a member rents a movie through Netflix, SeeYou will broadcast that information to everyone in the member’s online network. How can SeeYou avoid complaints that this program violates its members’ privacy? (See *Privacy*.)

Solution

Initially, SeeYou’s best option in this situation might be to give members the opportunity to prevent the broadcast of any private information by requiring their consent. Otherwise, the members could legitimately complain that the new program was causing publication of private information without their permission. Or SeeYou might allow members to affirmatively opt out of the program altogether. Of course, SeeYou might also discontinue the program. And if any of the members decide to file a suit against SeeYou for violations of federal or state privacy statutes, the firm might offer to settle to avoid further complaints and negative publicity.

1. **Copyrights in Digital Information.** When she was in college, Jammie Thomas-Rasset wrote a case study on Napster, an online peer-to-peer (P2P) file-sharing network, and knew that it had been shut down because it was illegal. Later, Capitol Records, Inc., which owns the copyrights to a large number of music recordings, discovered that “tereastarr”—a user name associated with Thomas-Rasset’s Internet protocol address— had made twenty-four songs available for distribution on KaZaA, another P2P network. Capitol notified Thomas-Rasset that she had been identified as engaging in the unauthorized trading of music. She replaced the hard drive on her computer with a new drive that did not contain the songs in dispute. Is Thomas-Rasset liable for copyright infringement? Explain. [*Capitol Records, Inc. v. Thomas-Rasset*, 692 F.3d 899 (8th Cir. 2012)] (See *Copyrights in Digital Information*.)

Solution

Yes, Thomas-Rasset is liable for copyright infringement. File-sharing is accomplished through peer-to-peer (P2P) networking. When file-sharing is used to download others’ stored music files, copyright issues arise. The issue of infringement in file-sharing has been a subject of debate since the cases against Napster, Inc. and Grokster, Ltd., two companies that created software used to share files in infringement of others’ copyrights. Napster operated a website with free software that enabled users to copy and transfer MP3 files via the Internet. Firms in the recording industry sued Napster. Ultimately, the court held Napster liable for copyright infringement.

Here, Thomas-Rasset willfully infringed Capitol’s intellectual property rights under the Copyright Act by making twenty-four songs available for distribution on an online peer-to-peer network. Her subsequent effort to conceal her actions by changing the hard drive on her computer showed a proclivity for unlawful conduct. This would support imposing an injunction on Thomas-Rasset against making songs or any recordings available for distribution to the public through a P2P or any other online media distribution system.

In the actual case on which this problem is based, Capitol filed a suit in a federal district court against Thomas-Rasset, who was found liable for copyright infringement and assessed damages of $54,000. On appeal, the U.S. Court of Appeals for the Eighth Circuit vacated the lower court's judgment, concluding that it should have assessed statutory damages of at least $222,000 and should have enjoined Thomas-Rasset from making copyrighted works available to the public. The appellate court remanded the case with directions to enter a judgment that included those remedies.

1. **Privacy.** Using special software, South Dakota law enforcement officers found a person who appeared to possess child pornography at a specific Internet protocol address. The officers subpoenaed Midcontinent Communications, the service that assigned the address, for the personal information of its subscriber. With this information, the officers obtained a search warrant for the residence of John Rolfe, where they found a laptop that contained child pornography. Rolfe argued that the subpoenas violated his “expectation of privacy.” Did Rolfe have a privacy interest in the information obtained by the subpoenas issued to Midcontinent? Discuss. [*State of South Dakota v. Rolfe*, 825 N.W.2d 901 (S.Dak. 2013)] (See *Privacy*.)

Solution

No, Rolfe did not have a privacy interest in the information obtained by the subpoenas issued to Midcontinent Communications. The courts have held that the right to privacy is guaranteed by the U.S. Constitution’s Bill of Rights, and some state constitutions contain an explicit guarantee of the right. A person must have a reasonable expectation of privacy, though, to maintain a suit or to assert a successful defense for an invasion of privacy.

People clearly have a reasonable expectation of privacy when they enter their personal banking or credit card information online. They also have a reasonable expectation that online companies will follow their own privacy policies. But people do not a reasonable expectation of privacy in statements made on Twitter and other data that they publicly disseminate. In other words, there is no violation of a subscriber’s right to privacy when a third-party Internet provider receives a subpoena and discloses the subscriber’s information.

Here, Rolfe supplied his e-mail address and other personal information, including his Internet protocol address, to Midcontinent. In other words, Rolfe publicly disseminated this information. Law enforcement officers obtained this information from Midcontinent through the subpoenas issued by the South Dakota state court. Rolfe provided his information to Midcontinent—he has no legitimate expectation of privacy in that information.

In the actual case on which this problem is based, Rolfe was charged with, and convicted of, possessing, manufacturing, and distributing child pornography, as well as other crimes. As part of the proceedings, the court found that Rolfe had no expectation of privacy in the information that he made available to Midcontinent. On appeal, the South Dakota Supreme Court upheld the conviction.

1. **File-Sharing**. Dartmouth College professor M. Eric Johnson, in collaboration with Tiversa, Inc., a company that monitors peer-to-peer networks to provide security services, wrote an article titled “Data Hemorrhages in the Health-Care Sector.” In preparing the article, Johnson and Tiversa searched the networks for data that could be used to commit medical or financial identity theft. They found a document that contained the Social Security numbers, insurance information, and treatment codes for patients of LabMD, Inc. Tiversa notified LabMD of the find in order to solicit its business. Instead of hiring Tiversa, however, LabMD filed a suit in a federal district court against the company, alleging trespass, conversion, and violations of federal statutes. What do these facts indicate about the security of private information? Explain. How should the court rule? [*LabMD, Inc. v. Tiversa, Inc.*, 2013 WL 425983 (11th Cir. 2013)] (See *Copyrights in Digital Information*.)

Solution

The facts of this case indicate that the security of private information in any database accessible from the Web is weak. And this information can be easily shared with others through peer-to-peer networks, which allow users to place shared computer files in folders that are open for other users to search.

As part of the research for their article, Johnson and Tiversa searched the networks for data that could be used to commit medical or financial identity theft. On one of them, they found a document that contained the Social Security numbers, insurance information, and treatment codes for patients of LabMD, Inc. Tiversa notified LabMD of the find. LabMD appeared not to have willingly revealed this information because on learning of its exposure, the company filed a suit against Tiversa.

In the actual case on which this problem is based, the court dismissed the suit for lack of personal jurisdiction over Tiversa. On appeal, the U.S Court of Appeals for the Eleventh Circuit affirmed. LabMD asserted jurisdiction under a long-arm statute of Georgia. But Tiversa was not registered to do business in Georgia, had no employees or customers in Georgia, derived no revenue from business activities in Georgia, owned no Georgia property, and paid no Georgia taxes. Furthermore, although accessible in Georgia, Tiversa’s website merely advertised its services, and did not offer products or services for purchase online. Tiversa's entire contact with Georgia consisted of one phone call and nine e-mails to LabMD. This was not sufficient.

1. **Business Case Problem with Sample Answer—Social Media.** Mohammad Omar Aly Hassan and nine others were indicted in a federal district court on charges of conspiring to advance violent jihad (holy war against enemies of Islam) and other offenses related to terrorism. The evidence at Hassan’s trial included postings he made on Facebook concerning his adherence to violent jihadist ideology. Convicted, Hassan appealed, contending that the Facebook items had not been properly authenticated (established as his own comments). How might the government show the connection between postings on Facebook and those who post them? Discuss. [*United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014)] (See *Social Media*.) **—For a sample answer to Problem 8–5, go to Appendix E.**

Solution

As stated in the text, law enforcement can use social media to detect and prosecute suspected criminals. But there must be an authenticated connection between the suspects and the posts. To make this connection, law enforcement officials can present the testimony or certification of authoritative representatives of the social media site or other experts. The posts can be traced from the pages on which they are displayed and the accounts of the “owners” of the pages to the posters through Internet Protocol (IP) addresses. An IP address can reveal the e-mail address, and even the mailing address, of an otherwise anonymous poster.

The custodians of Facebook, for example, can verify Facebook pages and posts because they maintain those items as business records in the course of regularly conducted business activities. From those sources, the prosecution in Hassan’s case could have tracked the IP address to discover his identity.

In the actual case on which this problem is based, on Hassan’s appeal of his conviction, the U.S. Court of Appeals for the Fourth Circuit affirmed.

1. **Social Media.** Kenneth Wheeler was angry at certain police officers in Grand Junction, Colorado, because of a driving-under- the-influence arrest that he viewed as unjust. While in Italy, Wheeler posted a statement to his Facebook page urging his “religious followers” to “kill cops, drown them in the blood of their children, hunt them down and kill their entire bloodlines” and provided names. Later, Wheeler added a post to “commit a massacre in the Stepping Stones Preschool and day care, just walk in and kill everybody.” Could a reasonable person conclude that Wheeler’s posts were true threats? How might law enforcement officers use Wheeler’s posts? Explain. [*United States v. Wheeler*, 776 F.3d 736 (10th Cir. 2015)] (See *Social Media*.)

Solution

Yes, a reasonable person could conclude that Wheeler’s posts were “true” threats. Law enforcement uses social media to detect and prosecute criminals. Police may also use social media to help them to locate a particular suspect or to determine the suspect’s identity.

In this problem, Kenneth Wheeler was angry at police officers in Grand Junction, Colorado, due to a driving-under-the-influence arrest that he viewed as a set-up. While in Italy, Wheeler posted a statement to his Facebook page urging his “religious followers” to “kill cops, drown them in the blood of their children, hunt them down and kill their entire bloodlines” and provided names. Later, Wheeler added a post to “commit a massacre in the stepping stones preschool and day care, just walk in and kill everybody.” In determining whether a “true” threat has been made, a court asks whether those who hear or read the threat reasonably consider that an actual threat has been made. Exhortations to unspecified others to commit violence can amount to true threats, so as to support a criminal prosecution based on those threats, especially if a reasonable person might believe the individuals ordered to take violent action are subject to the will of the threatening party. Law enforcement officers might use Wheeler’s posts to detect, investigate, and prosecute any crimes. Police may also use the posts to help them to determine Wheeler’s identity and his location.

In the actual case on which this problem is based, Wheeler was convicted of transmitting a threat and sentenced to forty months' imprisonment. On appeal, the U.S. Court of Appeals for the Tenth Circuit held that a reasonable person could interpret Wheeler’s statements to be “true” threats. The court remanded the case for a new trial on other grounds.

1. **Social Media.** Irvin Smith was charged in a Georgia state court with burglary and theft. Before the trial, during the selection of the jury, the state prosecutor asked the prospective jurors whether they knew Smith. No one responded affirmatively. Jurors were chosen and sworn in, without objection. After the trial, during deliberations, the jurors indicated to the court that they were deadlocked. The court charged them to try again. Meanwhile, the prosecutor learned that “Juror 4” appeared as a friend on the defendant’s Facebook page and filed a motion to dismiss her. The court replaced Juror 4 with an alternate. Was this an appropriate action, or was it an “abuse of discretion”? Should the court have admitted evidence that Facebook friends do not always actually know each other? Discuss. [*Smith v. State of Georgia*, 335 Ga.App. 497, 782 S.E.2d 305 (2016)] (See *Social Media*.)

Solution

The action by the court in replacing Juror 4 with an alternate was not an abuse of discretion. Nor did the court err in not admitting evidence that in general Facebook friends do not always actually know each other.

In this problem, Smith was charged with burglary and theft by taking a motor vehicle. Before the trial, during voir dire—the selection of the jury panel— the state prosecutor asked the prospective jurors, whether they knew Smith. No one indicated that they did. Jurors were chosen and sworn in, without objection. After the trial, during deliberations, the prosecutor learned that “Juror 4” appeared as a friend on Smith’s Facebook page and filed a motion to dismiss her from the jury. The court granted the motion and replaced Juror 4 with an alternate. This was not an abuse of the court’s discretion because Juror 4 was connected to Smith in some way and her failure to disclose the connection during voir dire placed in doubt her ability to determine his guilt or innocence impartially.

As for whether evidence should be admitted to the effect that Facebook friends might not actually know each other, it would not be abuse of discretion to exclude it. Such evidence would not relevant to Juror 4’s unique situation, her “personal style”—that is, whether she actually knew the defendant and if so, in what way.

In the actual case on which this problem is based, after the juror was replaced with an alternate, the jury returned a guilty verdict. A state intermediate appellate court affirmed this result, after a review of the issues focused on here.

1. **Internet Law.** Jason Smathers, an employee of America Online (AOL), misappropriated an AOL customer list with 92 million screen names. He sold the list for $28,000 to Sean Dunaway, who sold it to Braden Bournival. Bournival used it to send AOL customers more than 3 billion unsolicited, deceptive e-mail ads. AOL estimated the cost of processing the ads to be at least $300,000. Convicted of conspiring to relay deceptive e-mail in violation of federal law, Smathers was ordered to pay AOL restitution of $84,000 (treble the amount for which he had sold the AOL customer list). Smathers appealed, seeking to reduce the amount. He cited a judgment in a civil suit for a different offense against Bournival and others for which AOL had collected $95,000. Smathers also argued that his obligation should be reduced by restitution payments made by Dunaway. Which federal law did Smathers violate? Should the amount of his restitution be reduced? Explain. [*United States v. Smathers*, 879 F.3d 453 (2d. Cir. 2018)] (See *Internet Law*.)

Solution

Smathers was charged with, and convicted of, violating the federal CAN-SPAM Act. This law applies to the sending of unsolicited “junk” e-mail, prohibiting the use of false, misleading, or deceptive information.

Smathers, an employee of America Online (AOL), misappropriated an AOL customer list with 92 million screen names. He sold the list for $28,000 to Sean Dunaway, who sold it to Braden Bournival. Bournival used it to send AOL customers more than 3 billion unsolicited, deceptive e-mail ads. AOL estimated the cost of processing the ads to be at least $300,000. Smathers was convicted of conspiring to relay deceptive e-mail in violation of the CAN-SPAM Act, which applied to the sending of the ads.

Smathers was ordered to pay AOL restitution of $84,000. He sought to reduce this amount by citing a judgment in a civil suit against Bournival and others for which AOL had collected $95,000. He also argued that the amount should be reduced by restitution payments made by Dunaway. As indicated by the facts, however, he was not a party to the Bournival litigation, which involved a different offense. And AOL’s total loss was at least $300,000. Payments by Smathers and Dunaway together are not likely to reach that figure, much less the $84,000 that Smathers was ordered to pay.

In the actual case on which this problem is based, the U.S. Court of Appeals for the Second Circuit affirmed the restitution order, concluding that Smathers’s contentions were “without merit.”

1. **A Question of Ethics—The IDDR Approach and Social Media.** One August morning, around 6:30 a.m., a fire occurred at Ray and Christine Nixon’s home in West Monroe, Louisiana. The Nixons told Detective Gary Gilley of the Ouachita Parish Sheriff’s Department that they believed the fire was deliberately set by Matthew Alexander, a former employee of Ray’s company. Ray gave Alexander’s phone number to Gilley, who contacted the number’s service provider, Verizon Wireless Services, L.L.C. Gilley said that he was investigating a house fire that had been started with the victims inside the dwelling, and wanted to know where the number’s subscriber had been that day. He did not present a warrant, but he did certify that Verizon’s response would be considered an “emergency disclosure.” [*Alexander v. Verizon Wireless Services, L.L.C*., 875 F.3d 243 (5th Cir. 2017)] (See *Social Media*.)

1. Using the Inquiry and Discussion steps in the IDDR approach, identify the ethical dilemma that Verizon faced in this situation and actions that the company might have taken to resolve that issue.

Solution

The ethical dilemma that Verizon faced in this case is whether to provide a police officer with the information that he asked for. With no warrant or other court order, Verizon had a substantial legal basis to refuse. If disclosure had been legally required, however, would the company have had an ethical basis to refuse? Or, did the company have an ethical obligation to respond, regardless of whether it was legally required to do so?

The IDDR approach begins with an Inquiry that sets out the ethical dilemma and identifies the stakeholders and the relevant ethical standards in a set of facts. The Discussion step covers actions to address the issue, the actions’ strengths and weaknesses, and their consequences and effects.

Here, Ray and Christine Nixon told Sheriff’s Detective Gary Gilley that they believed a fire in their home had been set by Matthew Alexander. Ray gave Alexander’s phone number to Gilley, who contacted the number’s service provider, Verizon. Gilley said that he was investigating a house fire that may have intentionally started with the victims inside, and wanted to know where the number’s subscriber had been that day. He did not present a warrant, but he did certify that Verizon’s response would be considered an “emergency disclosure.”

The stakeholders in this situation include all of the immediate parties—the Nixons, Alexander, Gilley, and Verizon—as well as other police officers, service providers, the public generally, and most importantly other potential victims if in the fact the fire had been arson.

Verizon can choose to reveal all of its information concerning its subscriber, none of the data, or some part of it. This choice might be affected by the company’s guidelines on what information to reveal, whom it may be disclosed to, and when it should be released. It might also be influenced by an altruistic motive to help others in distress (the NIxons), in need (the police), or in harm’s way (unwitting potential victims). There may also be a perceived overriding ethical duty to protect privacy rights.

The strengths and weaknesses of the actions exist in their consequences. Refusing to disclose the information could protect the privacy of Verizon’s subscribers, and ultimately, contribute to the protection of the privacy for all. But it would impede a police investigation of a possible crime, which could result in the Nixons or others being further victimized. Disclosing all, or at least some, of the information could prevent the negative consequences of revealing none of it. Relying on the detective’s “certification” that this response would be considered an “emergency disclosure” would lend moral, and possibly legal, support to this decision. Finally, revealing only where the subscriber had been that day, without disclosing content (no texts, e-mails, or conversations), could arguably protect privacy rights.

2. Suppose that Verizon gave Gilley the requested information, and that later Alexander filed a suit against the provider, alleging a violation of the Stored Communications Act. Could Verizon successfully plead “good faith” in its defense?

Solution

Yes, if Verizon gave Gilley the requested information, and later Alexander filed a suit against the company, under the Stored Communications Act (SCA), the defendant could successfully plead “good faith” in its defense.

The SCA prohibits the intentional and unauthorized access to stored electronic communications. The act also prevents providers of communications services from disclosing private communications to certain entities and individuals. There are civil sanctions for violations. Thus, in the circumstances of this case, as a provider, Verizon might violate the act by responding to Gilley’s request with the information that he sought—where the subscriber to a certain phone number had been that day.

Gilley did not present Verizon with a warrant, but he stated the purpose for his request and certified that the provider’s response would be considered an “emergency disclosure.” The company could believe in good faith, then, that an emergency involving a risk of serious injury or other harm to a person mandated the disclosure of the data. This would most likely serve as a sufficient legal defense to a suit by the party whose information was disclosed.

In ethical terms, as related in the answer to the question above, there are also significant altruistic and other moralistic reasons to support the disclosure of the information.

In the actual case on which this problem is based, Verizon provided Gilley with the information. Alexander was charged in a Louisiana state court with arson. The court suppressed the records obtained from Verizon, finding no exigent circumstances to justify Gilley acting without a warrant.

Alexander filed a suit in a federal district court against Verizon, alleging a violation of the SCA. The court dismissed the suit. The U.S. Court of Appeals for the Fifth Circuit affirmed the dismissal. “Verizon acted reasonably in concluding that there was an emergency .  .  . that required Verizon to act without delay.”

Critical Thinking and Writing Assignments

1. **Time-Limited Group Assignment—File-Sharing.** James, Chang, and Braden are roommates. They are music fans and frequently listen to the same artists and songs. They regularly exchange MP3 music files that contain songs from their favorite artists. (See *Copyrights in Digital Information*.)
2. One group of students will decide whether the fact that the roommates are transferring files among themselves for no monetary benefit protects them from being subject to copyright law.

Solution

Just because the three roommates are not profiting from their file-sharing actions does not mean that they wouldn’t be subject to copyright law. A copyright violation can occur in the absences of any monetary benefit. Congress extended liability under copyright law to persons who exchange unauthorized copyrighted words without realizing a profit.

1. The second group will consider whether it would be legal for each roommate to buy music on CD and then, after downloading a copy on to their hard drive, give the CD to the other roommates to do the same. Does this violate copyright law? Is it the same as file-sharing digital music? Explain.

Solution

The purchaser of a CD has the right to loan or sell that CD to anyone else. If the roommates each rip the CD to their own hard drives, generally, there will be no copyright violation.

1. A third group will consider streaming music services. If one roommate subscribes to a streaming service and the other roommates use the service for free, would this violate copyright law? Why or why not?

Solution

If one roommate subscribes to a streaming service and the other roommates use the service for free, this would violate copyright law if it violates the terms of the service agreement or the service’s policy.

Copyright is the most important form of intellectual property protection on the Internet. Because most, if not all, of the material is copyrighted, simply transferring it online is copying it in violation of copyright law. Thus, sharing the stored music files of others, especially those of the owner of the copyright to the music, raises copyright issues. Some companies have aggressively pursued who shared the firms’ property. Others have not, perhaps to avoid bad publicity or to attract new customers.

If the streaming service in the question opposes the sharing of its service, then doing so clearly infringes on the company’s copyrights. This is both a criminal and a civil violation of copyright law. Penalties and sanctions include damages and injunctions. A user might argue the innocent infringer defense—being unaware that the actions constituted copyright infringement. The application of these principles is for the determination of a court.

Of course, if a steaming service turns a blind eye to the sharing of its material, there are not likely to be negative consequences to those who do it.