*Teaching Case*

# Ethical Coding: Privacy, Ethics & Law in Computing

Christine Ladwig
cladwig@semo.edu
Department of Marketing

Dana Schwieger
dschwieger@semo.edu
Department of Management

Southeast Missouri State University
Cape Girardeau, MO 63701, USA

## Abstract

This case provides an opportunity for classroom discussion of ethical issues addressed by computing technologists and the Association of Computing Machinery (ACM) Code of Ethics as the authors describe a recent lawsuit brought against Sutter Health. Security issues, data breaches and compliance with industry privacy rules are common concerns for all industry professionals, including computing technologists. However, employer work requests—of questionable moral position—place employees in ethical dilemmas that add another layer to job-related stress. This case may be used in a graduate level management information systems course or as part of a capstone class experience. Suggested assignments include discussion questions regarding the ACM Code of Ethics and the right to privacy, and situational ethics scenarios for programmers.

Keywords: Teaching Case, ACM Code of Ethics, Privacy Law

## 1. INTRODUCTION

As companies increasingly realize the value of data analytics, computing technologists may be asked to enhance their programs and systems with data collection capabilities unassociated with the intended purpose of the resource. While users of the technology tool may assume that their data is being used only for the activity at hand, in reality, their data may actually be collected and used beyond the implied purpose of the system. Computing technologists need to be aware of laws and industry codes of ethics as they develop programs. In addition, future technologists should also be aware that they may be placed in situations where their ethical values may need to guide and direct their decision making. They may also want to be prepared to think about how they would handle a situation in which their employer or co-worker's ethical intentions are questionable.

There is some guidance available to assist computer technologists in applying industry ethical principles. The world's largest computing organization—the Association for Computing Machinery (ACM)—updated their ethics code in 2018 due to the significant advances in technology. The group's ethics standards had last been updated in 1992. The ACM Code of Ethics is regarded as the standard for the computing profession and is designed to guide computer technologists in making ethically responsible decisions to "ensure the public good." (ACM, 2019). This case focuses on the law and ethics of data sharing. The handling of

healthcare data is especially sensitive; and therefore, our study of legal and ethical situations begins with an action filed against a major healthcare provider for sharing confidential information with third parties.

## 2. THE LAWSUIT

On Monday, June 10, 2019, a class action lawsuit (*Jane Doe I and Jane Doe II v. Sutter Health*) was filed in Sacramento County, California against Sutter Health. Sutter Health is one of California's largest health care providers with 24 hospitals serving more than 100 northern California communities. The lawsuit claims that Sutter secretly shared private information about patients with Facebook, Google, Twitter, LinkedIn, as well as other companies. The claim indicates source code was written into the website that allowed for "cookie synching" and the provision of a "… secret and invisible window through which to spy on the communications that the Defendant exchanges with its patients." (*Jane Doe I and Jane Doe II v. Sutter Health*, 2019). According to the claim, the window was indicated by a third-party logo (i.e. Facebook "share" icon) present on the page or a one-by-one tracking pixel. The claim noted that a GET request would disclose the subject matter of a search. Personally identifiable information was also supposedly disclosed including cookies, the IP address, and device and browser identifiers. Javascript code was indicated as being used in the web page to allow a first-party cookie value stored in a tracking pixel to be shared with third-party partners allowing for "cookie synching." (Cookie synching allows two web sites to share data collected about individual users.) This data was supposedly included in the development of detailed dossiers used to target advertising to both current and potential Sutter patients (Cahill, 2019).

If these allegations are true, then Sutter Health may not only have violated laws intended to protect privacy; but may also have committed ethical transgressions. The next section describes protected health information.

## 3. PROTECTED HEALTH INFORMATION

Protected health information (PHI) is individually identifiable health information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HIPAA Journal describes PHI to include such things as "health records, health histories, lab test results, medical bills, demographic information, and common identifiers when they can be linked with health information." However, when PHI is stripped of identifiers that can link individuals to the information, the information is described as being de-identified and PHI HIPAA rules do not apply. The next section provides a summary of the alleged legal violations

## 4. VIOLATIONS

The class action lawsuit includes complaints for the following issues:

1. Violation of California Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56, et seq.)
2. Violation of California Invasion of Privacy Act (Cal. Penal Code §§ 631, et seq.)
3. Intrusion upon Seclusion
4. Breach of Fiduciary Duty of Confidentiality
5. Violation of California's Unfair Competition Law (Cal. Bus. Prof. Code §§ 17200, et seq.)
6. Conversion
7. Negligence

The following provides a short explanation of each of the complaints included in the lawsuit with the accompanying allegations. Several of the complaints refer to the term "tort" which is defined as an act or omission that causes harm or injury to another.

Violation of California Confidentiality of Medical Information Act (Cal. Civ. Code §§ 56, et seq.): This act indicates that health care providers cannot disclose patient medical information without the patient's consent. According to the law, medical information also includes information that could identify the person as being a patient of the facility. (*Jane Doe I & Jane Doe II v. Sutter Health*, 2019).

Violation of California Invasion of Privacy Act (Cal. Penal Code §§ 631, et seq.): This act protects internal communications from being shared without the consent of the parties involved. The claim indicates that the sharing of communications with third-party entities violates this act (*Jane Doe I & II v. Sutter Health*, 2019).

Intrusion upon Seclusion is a privacy tort associated with intruding upon the private affairs of another person (Duhaime, 2019). The lawsuit alleges that the disclosure of medical communications and personally identifiable information violates this tort (*Jane Doe I & Jane Doe II v. Sutter Health*, 2019).

Breach of Fiduciary Duty of Confidentiality Healthcare providers have a heightened responsibility to protect the personal and medical information of their patients. The lawsuit against Sutter Health alleges that the company breached their fiduciary duty to keep communications between them and their patients confidential by transmitting browsing experiences of users to third parties, without consent (*Jane Doe I & Jane Doe II v. Sutter Health*, 2019).

**Violation of California's Unfair Competition** Law (Cal. Bus. Prof. Code §§ 17200, et seq.): This law prohibits fraudulent, deceptive or misleading business practices. The complaint alleges that Sutter Health violated this law through "misrepresentations and omissions regarding the disclosures of the personally identifiable information to third-parties…" (*Jane Doe I & Jane Doe II v. Sutter Health*, 2019).

The Conversion tort applies to taking someone's personal property without permission. (DMLP, 2019). The case alleges that Sutter Health "stole" web site users' confidential information.

Negligence laws are intended to protect people from injuries by others who may be careless or reckless. According to the suit filed against Sutter Health, the company had a duty to maintain the confidentiality of their users'/patients' personal and medical information, and not share their data with third parties without permission.

Like almost all companies that collect data from users, Sutter Health has a privacy policy linked to their web site for users to read before using the site. This document contains multiple sections and subsections detailing the collection of personal user information on their site. (Relevant Sections from the privacy document can be found in Appendix 1.) The document also indicates that the collection will occur in multiple ways.

The privacy policy informs users how their data may be collected and how it may be used. When the case goes to court, the content of the privacy policy will be evaluated. The court may find no fault with Sutter's actions. However, even though policies may make some actions legal, that does not necessarily mean that all legal actions are ethical. The next section examines the ethical aspect.

## 5. LAW AND ETHICS IN COMPUTING

When considering the law and programmer's code of ethics, the Sutter Health case is a good example of the potential risks that may be encountered even in the most seemingly mundane and straight-forward computing work assignments. Computer technologists must consider the intended, and even unintended, consequences of their work in the internet environment, and keep the tenets of privacy (Schwieger & Ladwig, 2016) and ethical programming—such as maintaining transparency and minimizing negative repercussions—at the forefront of every assignment.

Most professional careers have some form of code of ethics (e.g., CPA, physicians, lawyers and computing). For those without a formal written code, moral responsibility, human decency and the Golden Rule (treat others the way you want to be treated), should, at the very least, hold sway. The code of ethics associated with the field of computer technology is the Association of Computing Machinery (ACM) Code of Ethics. This document can provide guidance to programmers professionally beyond their own personal code of ethics. An excerpt from the ACM Code of Ethics can be found in Appendix 2.

Following the right ethical path is not always as easy as one would think. In his article "Ethical Dilemmas Faced by Software Engineers" (July 13, 2019) Princeton University author and computer scientist Arvind Narayanan discusses some real-life examples of ethics situations in computing. One of the contributors to the article mentions that although the issue of privacy has subtle implications for software engineers, the topic doesn't get much attention because there "are not enough dead bodies." Computer programmers must realize that unethical programming is not just a management issue. Students should understand and apply legal and ethical principles to their daily work and projects. (Narayanan, 2019).

## 6. ASSIGNMENTS

Faculty may use this exercise to address technology-related basic business law issues, familiarize students with the ACM Code of Ethics, and consider examples of circumstances where knowledge and consideration of ethics is vital for computer programmers. Discussion of answers for assignments are provided in the teaching notes.

Questions for Discussion
Courses: Graduate level MIS course or Capstone MIS Course

1. Visit the ACM's Code of Ethics Website and read through the Code (https://www.acm.org/code-of-ethics). After reading the Code, answer the following questions:

1. Do you think it is ethical to use someone's data for unintended purposes without their consent?
2. Assume that your supervisor asks you to add code to your project to collect data from unsuspecting users and to transfer that data to third parties (as allegedly occurred in the Sutter Health case). What would you do?
3. Assume you are a supervisor. What would you do if your employer asked you to have your employees add data collection code to the project on which they were working?
4. Does your opinion change as your roles change?

2. We do not yet know what the programmers of the Sutter Health site understood about the legal and ethical aspects of the company's website design. In each of the following situations, imagine you are a computer programmer asked to complete the described work assignment by your employer. Study the following scenarios and decide on a course of action. To evaluate the ethics of each situation, you can use the following ethical decision-making model:

(1) describe the ethical dilemma;
(2) identify the stakeholders;
(3) outline your options and how each group of stakeholders will be affected;
(4) make a decision among the options you've identified.

After you've developed a strategy/made a decision, examine the ACM Code of Ethics. Does your action align with the Code? Why or why not?

a. You are asked by your employer, a pharmaceutical company, to design a website to promote a drug they have developed. Federal law prohibits direct medical marketing to consumers at this time, so the company asks you to design the general information site as an online quiz, where users do not know it relates to the drug company. The target audience is teenaged girls. When taking the quiz, participant answers may vary, but the site always recommends the same drug (your company's target product). Sometimes the drug may be harmful to the user, depending on how they answer the quiz.

b. You are asked by your employer, a company that builds and programs self-driving cars, to design the "object avoidance" feature of the vehicles. You currently need to determine what the car will collide with when sandwiched between a stationary object (which could injure/kill the vehicle occupants) and a human moving target, such as a bicyclist or motorcyclist. All you know is that there is the potential for someone to be injured or killed by the programming, and the car needs to hit one of the two targets.

c. You are asked by your employer, a major clothing brand retailer that focuses on one gender, to program a competition on their website for entrants to win prizes, such as an iPhone. The company also asks you to write code to extract five random winners. Management, however, only wants winners to come from the targeted gender.

## 7. SOURCES

ACM (2019). ACM Code of Ethics and Professional Conduct. Retrieved on June 20, 2019 from https://www.acm.org/code-of-ethics

Cahill, N. (2019). Patients Claim Health Care Provider Shares Private Info with Tech Companies. *Courthouse News Service*, Retrieved on June 20, 2019 from https://www.courthousenews.com/patients-claim-health-care-provider-shares-private-info-with-tech-companies/

DMLP - Digital Media Law Project (2019). Retrieved on June 20, 2019 from http://www.dmlp.org/

Duhaime's Legal Dictionary (2019). Retrieved on June 20, 2019 from http://www.duhaime.org/LegalDictionary.aspx

HIPAA Journal (2017). What is Considered PHI Under HIPAA? Retrieved on March 27, 2020 from https://www.hipaajournal.com/considered-phi-hipaa/

*Jane Doe I and Jane Doe II v. Sutter Health*, Superior Court of California, 2019. Retrieved on June 20, 2019 from : https://www.courthousenews.com/wp-content/uploads/2019/06/Sutter.pdf

Narayanan, A. Ethical Dilemmas Faced by Software Engineers. (July 13, 2019). Retrieved on July 13, 2019 from https://freedom-to-tinker.com/2013/09/04/ethical-dilemmas-faced-by-software-engineers-a-roundup-of-responses/.

Schwieger, D., Ladwig, C. (2016). Protecting Privacy in Big Data: A Layered Approach for Curriculum Integration. *Information Systems Education Journal,* 14(3) pp 45-54. http://isedj.org/2016-14/ ISSN: 1545-679X.

Sutter Health (2019). Privacy Policy. Retrieved on June 20, 2019 from https://www.sutterhealth.org/privacy-policy.

Simulation of the ethics of self-driving cars. *Moral Machine*, Retrieved on July 13, 2019 from http://moralmachine.mit.edu/.

## APPENDICES

### APPENDIX 1: SUTTER **HEALTH'S PRIVACY AGREEMENT**

Linked to the homepage of Sutter Health's web site is the address to Sutter's Privacy Policy with multiple sections and subsections. Areas of the document containing content relevant to this article include:

- Collection of Personal Information
- Web Site Visitor Tracking
  - Visitor Tracking Software
  - Web Logs
  - Internet Cookies
- Use and Disclosure of Personal Information

The following subsections provide excerpts from the Privacy Policy document that could be considered relevant to the case.

Collection of Personal Information: In the section entitled "Collection of Personal Information," the page notes:

> *"Sutter collects information about you, and sometimes about your devices, when you visit our Sites. The information we collect and how we collect that information may vary depending on the specific website or application. The information we collect about you through our Sites generally is information that you provide or information that we automatically collect…. We also collect information about you, and sometimes about your computer or device, automatically through cookies and other technology. … In some cases, we may collect location information from you, including your precise location, if you have enabled this functionality for Sites. Most mobile devices allow you to change or disable this functionality by changing the device settings. We also may collect information regarding how you interact with our Sites and on other websites, such as our social media platforms. … In some cases, we may receive information about you from third parties. Once we receive this information, we will use, disclose, and safeguard it as described in this Policy. We may combine information collected through different Sites or portions of Sites. In the event we combine personal information collected through our Sites with your personal health information, we will use and disclose such combined information as described in our Notice of Privacy Practices, which relates to our collection, use, and disclosure of medical information."* *(SutterHealth.org, 2019).*

Visitor Tracking Software: The content, in the Visitor Tracking Software section of the site, notes:

> *"Sutter keeps track of visits to our Sites via an automatic monitoring program that tells us, among other things, how many visits are made to the site; the time of day and date of those visits; and which areas of the Sites individuals visited. The monitoring program does not provide us with any personal information about a visitor. We cannot discern your name or physical address or other personal information about you. This information is used to evaluate the effectiveness of our Sites."*

The paragraph indicates that the physical address cannot be discerned; however, reverse IP lookup software may be able to provide users' locations.

Web Logs: The section of the page entitled "Web Logs" describes the data that is stored regarding site visits:

> *"The visitor tracking software gathers information from standard Web logs and stores it on servers at Sutter. These logs may contain information such as the Internet domain from which you access our Sites; the date and time you visited our Site; the areas of our site that you viewed; your computer's IP address that is automatically assigned when you log onto the*

> *Internet; the type of browser and operating system you use; and the address of the Web site you linked from, if any.*
>
> *All Web logs are stored securely and may only be accessed by Sutter employees or designees on a professional need-to-know basis for a specific purpose. Sutter uses Web log information to help us design our Sites; identify popular features; resolve user, hardware and software problems; and make the site more useful to patients and other visitors."*

The Internet Cookies section describes the types of cookies that are used as well as how cookies are used.

> *Sutter may place Internet "cookies" on the computer hard drives of visitors to our Sites. Cookies help us obtain information about your use of our Sites; they do not contain information about you or your health history. Sutter uses two types of cookies: "session" cookies and "persistent" cookies*
>
> *…Some of our Sites may use Google Analytics to better understand usage of our Sites. You may opt out of Google Analytics by following the instructions at: https://tools.google.com/dlpage/gaoptout. Additionally, you may opt out of certain tracking by many third party advertisers, by following the instructions found on the following Web sites: Network Advertising Initiative, http://optout.networkadvertising.org and Digital Advertising Alliance, http://optout.aboutads.info .*
>
> The collection, use, and disclosure of your information, as described in this Policy, may continue regardless of whether or not you enable "Do Not Track" functionality on your browser or device.

Use and Disclosure of Personal Information: The final section relating to the case notes:

> *We may use your information: to contact you … to track and analyze use of our Sites, … and to track and evaluate activity on our Sites; for purposes including enhancing and maintaining our Sites, services, and products; …*
>
> *We may share information that does not specifically identify you, such as aggregate data, with third parties. Additionally, we may share your information, including your personal information collected through our Sites, under the following circumstances: with our third party service providers who perform certain services or functions on our behalf (for example, we may share your information with a hosting service provider who hosts one of our Sites that you have visited);…*

## APPENDIX 2: ACM CODE OF ETHICS

The Association of Computing Machinery's (ACM) Code of Ethics and Professional Conduct should serve as a guide for current, and future, computing practitioners. The Code, found at https://www.acm.org/code-of-ethics, is divided into four main sections: (1) General Ethical Principles, (2) Professional Responsibilities, (3) Professional Leadership Principles, and (4) Compliance with the Code (ACM, 2019).

Although upholding privacy and data security are woven throughout the document, the section entitled "General Ethical Principles" most obviously addresses the issue of privacy with five of its seven subsections related to the topic.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing: The focus of this subsection centers upon looking out for others. The subsection notes, "This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority." (ACM, 2019).

1.2 Avoid Harm: This subsection of ACM's Code of Ethics addresses user privacy, and the responsibility of a computing professional, most substantially. "In this document, "harm" means negative consequences, especially when those consequences are significant and unjust. Examples of harm include unjustified physical or mental injury, unjustified destruction or disclosure of information, and unjustified damage to property, reputation, and the environment. This list is not exhaustive. Well-intended actions, including those that accomplish assigned duties, may lead to harm" (ACM, 2019).

1.3 Be honest and trustworthy: The focus of this subsection centers upon the disclosure of system and personal capabilities to employers. Although this subsection does not address user privacy directly, the subsection emphasizes the importance of being honest and trustworthy in action and deed. "Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code" (ACM, 2019).

1.6 Respect privacy: This subsection of the document reminds professionals that "Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected." and encourages professionals to become familiar with the "…various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information (ACM, 2019)."

1.7 Honor confidentiality: The General Ethics Principles section wraps up with this subsection that reinforces the importance of privacy. "Computing professionals are often entrusted with confidential information such as trade secrets, client data,… Computing professionals should protect confidentiality…"