Journal of Information Systems Education

Volume 37
Issue 2
Spring 2026

Teaching Tip

Data Privacy in Business: Balancing Customer Trust and Data Insights

Soham Sengupta, Stephanie A. Totty, and Steven A. Morris

Recommended Citation: Sengupta, S., Totty, S. A., & Morris, S. A. (2026). Teaching Tip: Data Privacy in Business: Balancing Customer Trust and Data Insights. *Journal of Information Systems Education*, 37(2), 184-204. https://doi.org/10.62273/YIWA1365

Article Link: https://jise.org/Volume37/n2/JISE2026v37n2pp184-204.html

Received: June 25, 2025
First Decision: August 22, 2025
Accepted: November 5, 2025
Published: June 15, 2026

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 37(2), 184-204, Spring 2026
https://doi.org/10.62273/YIWA1365

Teaching Tip
Data Privacy in Business: Balancing Customer Trust and Data Insights

Soham Sengupta
Stephanie A. Totty
Steven A. Morris
Department of Information Systems & Analytics
Middle Tennessee State University
Murfreesboro, TN 37132, USA
soham.sengupta@mtsu.edu, stephanie.totty@mtsu.edu, steven.morris@mtsu.edu

ABSTRACT

Ethics is vital for information technology professionals as data-driven decision-making has become the norm. Model curricula and accreditors have noted the need for university students to be able to evaluate situations with ethical considerations. In this teaching tip, we developed a role-playing ethics case exercise that makes students consider the legal and ethical considerations surrounding collecting data and how organizations can address them. Students take on one of five stakeholder perspectives: the company collecting customer data, the customer, a third-party data broker, regulators, or hackers. This exercise enables students to get a more holistic understanding of the challenges and opportunities related to collecting customer data. The case study includes security and privacy background information, making it flexible enough to work in a wide variety of classes, including classes where students have a limited technical background. Evidence indicates that the case increased student awareness of data privacy issues and the varied stakeholders and their interests.

Keywords: Teaching tip, Ethics, Cybersecurity, Role-play, Teaching methods, Discussion group

1. INTRODUCTION

Ethics is included in IS curriculum standards, such as the MSIS 2016 Global Competency Model and the IS 2020 Curriculum (CC2020 Task Force, 2020), and in those of accrediting agencies such as AACSB (Association to Advance Collegiate Schools of Business) and ABET (Accreditation Board for Engineering and Technology, 2025). However, the need for additional development of ethics competency within information systems continues to be an issue (AlDhaen, 2025; Barry & Ohland, 2012; Brown et al., 2024). Of particular interest and need is the area of cybersecurity. Existing work has specifically addressed cyber ethics teaching activities involving the ethical implications of collecting customer data (e.g., Skirpan et al., 2018), which prompted the initial development of our technique. However, researchers have highlighted the need for more work in helping individuals expand the use of ethical concepts in a wider range of computing situations (Myyry et al., 2009; Siponen, 2001). Our case answers the call from other researchers to develop role-playing activities that can be personally applicable to students instead of abstract scenarios of operations within an industry or company (Avin et al., 2020; Hanschke et al., 2024; Widyasari, 2020).

To address this issue, we developed a technique that applies existing role-playing approaches to teaching ethics in a scenario that can be broadly applied to cybersecurity and many other areas in the IS curriculum, such as programming, systems analysis and design, databases, telecommunications, and analytics. The case may also be suitable for more generic business or ethics courses. Role-playing, a derivative of sociodrama (Blatner, 2009), is a pedagogical exercise (Maier, 2002; Sogunro, 2004) where students learn about real-world scenarios in a focused, efficient, and holistic manner. It involves students taking on unfamiliar roles within a structured scenario (Shapiro et al., 2021) where they are assigned the roles. Role-playing in education develops critical thinking and interpersonal skills while lowering performance anxiety for students as compared to other pedagogical techniques (Sogunro, 2004). This kind of dramatic improvisation, or first-person characterization, is an effective way to have students share and understand multiple perspectives (Howes & Cruz, 2009).

The technique described here centers around a brief case scenario of a problem with multiple facets. We added details to make the case seem realistic, engaging, and relatable. The case presents considerations and prompts for five different stakeholders in the scenario. Care was taken to ensure that the provided information and prompts remain neutral (Farhoomand, 2004). Therefore, the prompts do not offer value judgments or analysis of the situation.

A case narrative must balance providing enough information to promote thoughtful responses while remaining concise to avoid noise (Cappel & Schwager, 2002; Farhoomand, 2004). Therefore, the case is detailed enough to engage different perspectives, while brief enough to be easily modified to address additional stakeholders when adapted to different courses without creating logical inconsistencies within the scenario. The setting used for the ethical dilemma is based around a smartphone application and addresses data security and privacy issues since most students can easily relate to the idea of sharing private data with apps, such as apps for fast food discounts and store loyalty apps. The case presented uses an app from an automotive insurance company since it is an easily relatable context for most students. This allows the case to provide ample context to enable the students to mentally engage with the scenario while reducing the memory load to recall it.

Finally, the technique is designed to support a range of learning domains from the revised Bloom's Taxonomy (Anderson & Krathwohl, 2001). The level of learning objectives that are appropriate for the case can vary based on the time devoted to ethical considerations. As a standalone ethics presentation, the learning objectives for this case are as follows:

- LO1. Students will be able to distinguish between various actors threatening or safeguarding their personal data.
- LO2. Students will be able to critically analyze the ethical implications of personal data sharing.
- LO3. Students will be able to communicate concerns related to sharing personal data.

If previous ethical considerations have been presented in the class, this case can be used to support higher levels of learning, such as:

- LO4. Students will be able to justify the consumer costs in return for the benefits from sharing personal data.
- LO5. Students will be able to prioritize various efforts to reduce risks associated with sharing personal data.

In this presentation of the technique, we focus only on the use of the case as a standalone exercise without prior ethical discussions in the class.

In Section 2, we present the main case narrative. Section 3 includes the tasks and questions for the students. Next, we provide teaching suggestions for instructors in Section 4, including 1) background information, specifically a concise overview of information security concepts to establish a common baseline of understanding, 2) recommendations for delivery, and 3) a proposed assessment strategy. We propose solutions in Section 5. In Section 6, we report evidence for the effectiveness of the assignment.

Finally, we provide ideas for the possible future expansion of the case and conclude in Sections 7 and 8, respectively. Figure 1 provides a quick start guide for the case.

QUICK START
Time: 40 minutes
Roles: Company, customers, hackers, data brokers, and regulators
Room setup: Discussion format
Deliverables: Improved student learning about different perspectives on ethical use of data and privacy
Notes: Activity materials are available in the appendices

Figure 1. Case Quick Start Guide

2. CASE PROBLEM: DATA PRIVACY ETHICS

Setomo Insurance, an auto insurance company, has launched a new program called DriveCool to better serve its customers. Customers who enroll in the DriveCool will receive discounted insurance rates. For example, one customer received a $150 discount on a 6-month contract that was already market-appropriate.

After enrolling in the DriveCool program, the user installs an app on their phone and a company-provided Bluetooth-enabled IoT device in their vehicle. The IoT device must always be paired with the user's phone to obtain and report the driving-related data to the company. If the location sharing or Bluetooth is disabled at any time, the app will send numerous notifications to reenable location sharing or Bluetooth, respectively. Setomo Insurance may unenroll the user from the DriveCool program if the user disables location sharing or Bluetooth, disallowing them to enjoy the competitive rates.

The discount is very desirable for customers, but customers must provide the company with some of their personal information to receive the benefit.

3. CASE TASKS AND QUESTIONS

In this exercise, you will role-play as different stakeholders related to this scenario by discussing their perspectives regarding the driving-related data. The stakeholders include Setomo Insurance, the customers, hackers, data brokers, and regulators.

Setomo Insurance: As a member of the IT strategy team, how might Setomo Insurance use the data collected by the DriveCool program? Who in the company should have access to this data?

Customers: As a Setomo Insurance customer, why would some customers not want Setomo Insurance to have access to their driving-related data? Are there any particular types of customers who would be especially vulnerable if Setomo Insurance had their data? Could Setomo Insurance use the driving-related data in a way that would not be in the customers' best interests? What would happen if Setomo Insurance experienced a breach of the driving-related data?

Hackers: As a hacker, how could you gain access to the driving data collected by Setomo Insurance? Why might you want to access this data?

Data Brokers: As a third-party data broker company, what value lies in the driving-related data collected by Setomo Insurance? Who would be interested in purchasing such data?

Regulators: As regulators, what privacy protection laws and standards currently protect customer data? How are these laws and standards different in different circumstances? How can these laws and standards be improved?

4. TEACHING SUGGESTIONS

This case was developed to be used and was pre-tested in a 40-minute, in-person class setting. Students did not complete work related to the case and had not received any ethics instruction prior to the in-person session. We started by providing background information to students (described in section 4.1 below). Then we ran the role-play exercise as described in section 4.2. Finally, we provide suggestions for how to assess student performance on the learning outcomes in section 4.3. Supplemental materials are available in the appendices, such as our slides (Appendix A), a printable scenario handout (Appendix B), and printable half-sheet role cards (Appendix C).

4.1 Case Background: Introduction to Security and Privacy

Establishing a baseline of understanding is an important first step in the use of the case exercise. The critical issue is providing students with the information necessary to understand the benefits and risks of data sharing. However, there are many modes of presentation that are possible. In our testing with the case, we presented this background information via lecture (using the slides in Appendix A) and discussion. We have found this more effective than simply asking students to read the information and more interactive than a recorded video presentation. The following subsections represent the background information needed by the students. Each represents a much larger area of interest, and a cybersecurity or privacy course could easily devote significant class coverage to each of these topics. For the purposes of the case, only a minimum understanding of each is necessary since the focus is on ethics, not on designing security strategies.

4.1.1 Introduction to Privacy. Students are generally familiar with the concept of privacy, so a simple definition is sufficient. Privacy is an individual's fundamental right to be left alone without interference or intrusion. Any data that can help in identifying an individual can be considered personal data. For example, an individual's health data, whether medical records, work-related data, date of birth, and location data (e.g., home address) are considered private.

Young adults are increasingly comfortable with sharing many types of personal information online, perhaps due to a perception of having a degree of control over their online data (Bietz et al., 2019). Therefore, it is necessary to provide context regarding the risks of sharing personal information without prejudicing the ethical conclusions that students are expected to draw from the case. Today, it is important to safeguard the online personal information of an individual to prevent identity theft and varying forms of social engineering hacks that individuals are subjected to after sharing their personal information online.

Providing personal data is a common practice for most students, so they can often provide numerous justifications for providing that information. Generally, one would provide personal information to companies in anticipation of getting better services and products through reduced pricing, loyalty programs, and others. Ostensibly, businesses use customers' data to provide customized services, offers, and products to retain existing customers and attract new ones. In the current era of artificial intelligence and business analytics, businesses also use customers' personal data to train their machine learning models to accurately predict customer behavior, intending to add value to their services and products that surpasses that of their competitors. In essence, individuals sell their personal data in exchange for the financial, service, and convenience advantages offered by the company.

In a digitalized economy, data is currency. The primary purpose for collecting customers' information is to help the company provide the best services and products to that customer to influence spending. This is the use of personal data that organizations typically emphasize with customers. Additionally, the secondary use of personal data is to sell the data itself. With a customer's consent, the company can sell the collected data to marketing firms and other companies. Therefore, companies want to collect personal data to remain competitive and ensure sustainability.

Unfortunately, businesses often sell personal information for purposes other than those that are made clear to customers. Personal information about consumers is such a prized commodity that there is a huge

appetite for hoarding data by companies and data aggregators, also known as data brokers. This opportunity, combined with loose data regulations, allows businesses to use and sell personal data for other purposes.

Revenue generated through selling customer data impacts the bottom line, which businesses cannot ignore, no matter how unethical it may be, unless they are compelled to comply with data privacy regulations. For example, fast food companies may collect additional data on customers in exchange for deals and rewards, which, unless closely scrutinized, can lead to these companies selling the data to other companies or marketing firms.

4.1.2 Introduction to Security. In the context of information security (InfoSec), security protects data (electronic/digital, printed, or spoken) from unauthorized access and data breaches. Effective InfoSec measures are needed to prevent data leaks, identity theft, and other cybercrime consequential to consumers and organizations. Ensuring data security is necessary to protect a company's reputation, as data breaches can lead to diminishing brand value and loss of trust from existing and prospective customers and shareholders. Students need to be aware, however, that not all personal data sharing by companies is intentional. For example, data brokers can "scrape" public websites, such as job posting sites, to gather data about individuals.

Organizations adopt different strategies to uphold information security standards. However, an in-depth or exhaustive delineation of strategies is not required for the case. Students need only to have a few examples to get a feeling that there are strategies that companies can use to safeguard personal information. The following strategies are provided in an overview as background.

- Privacy by design (PBD): Companies adopt a strategy of proactively incorporating privacy as a core requirement during the design and development of services and products. This helps in ensuring maximum data privacy for customers as a default setting.
- Cookie preferences/consent: Companies can remove unwarranted third-party data brokers scraping data from across the web using APIs and other means.
- Privacy policies: Companies can update their privacy policies to maintain compliance with privacy regulations and provide visibility and transparency about their customers' data collection and storage.

The important takeaway for students in this area is that strategies exist and security is a reasonable goal for which organizations strive.

4.1.3 Stakeholders. The interests of the *company* and the *customers* have been discussed because they are the parties to the transaction to acquire personal data. Also, students tend to be familiar with the consumer and company roles. However, students need to be conscious of other ethical players in the realm of personal data exchanges.

One group is *hackers*. Hackers are anonymous entities (individuals or groups) that aim to obtain illegal access to electronic data, networks, and systems of desirable targets, mainly for financial gain. Hackers can be internal to the company or external. Internal hackers are employees who may have malicious intent or accidentally cause breakdowns in security measures. Disgruntled current or former employees might attempt to access the organization's digital infrastructure to harm the company's reputation and brand value. While not intentionally attempting to disrupt the company, well-meaning employees can also play a role in security risks through common actions like clicking on external links, which may make the company's electronic data safeguards brittle and vulnerable to outsider attacks.

External hackers are poised to cripple or disrupt the services of an organization or breach the privacy of individuals for some kind of gain, often financial but sometimes to tarnish the image of an individual or corporation, or to force action. These attacks can be technical in nature, by manipulating vulnerabilities in the information systems technology, or social in nature, by manipulating the users of the system. Social-based techniques that manipulate or trick individuals into divulging confidential information or performing actions to weaken security measures are referred to as social engineering and are a common technique for hacking.

Another group of stakeholders is *third-party data brokers*. Data brokers are data aggregators that collect data from various sources and aggregate it to build individual profiles and sell it to marketing companies. Registered data brokers are the legal entities that organizations hire to collect customer data for selling to other companies or to customize their services and products better. The data brokers must comply with the company's privacy policies and data protection regulations or lose their licenses. Unregistered data brokers are shadowy entities operating without jurisdiction. They crawl the internet through various means to aggregate detailed data about individuals without their knowledge or consent and sell it to the highest bidders. The data on individuals sold through these brokers is often used to architect social engineering attacks.

The final group of stakeholders is the *regulators*. Regulators are the gatekeepers who develop and enforce privacy-protecting rules. Violations will give the regulators the right to penalize the companies and revoke the data broker's license. The regulator's objective is to safeguard the consumer's data from being exploited by companies and other entities. To achieve that, they scrutinize companies' privacy policies to ensure they have the best interest of the consumer in mind while collecting their data. Regulators also strive to strike a balance between empowering consumers to have better control of their own data and the business's interests.

Regulators include a large number of organizations and government agencies tasked with finding a balance between trade and protecting individuals. Regulatory laws like the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), and regulatory bodies like the Federal Trade Commission (FTC), among many things, ensure the protection of consumers. They do so by enforcing laws regarding transparency and explicit consent of consumers before their data is collected, ensuring data security and accuracy, and establishing procedures for handling consumer requests about their data.

Regulators are aided by non-regulatory standards organizations, like the National Institute of Standards and Technology (NIST) and the International Organization of Standardization (ISO). NIST and ISO provide frameworks for companies to follow to better manage data privacy and comply with privacy regulations (International Organization for Standardization, 2024; National Institute of Standards and Technology, 2024).

4.2 Running the Role-Play Case

We assigned each student to a role: Setomo Insurance, customers, hackers, data brokers, or regulators. We adopted an adapted Think-Pair-Share learning strategy (Kaddoura, 2013). Think-Pair-Share begins by giving students time to consider their own thoughts about a problem or answers to questions (*think*). During the "Think" stage, students were asked to write down their own thoughts regarding the questions for their role to encourage active participation during this step. This output could be collected later for the assessment of individual students. Then, students *pair* with others in the class to compare responses. For the pair stage, we grouped students by role rather than pairing students to reduce the time needed during the share stage for large classes. During the "Pair" stage, the instructor walked around to each of the groups to listen and encourage discussion if students needed help. Finally, the pairs *share* their collaborations with the class. During the "Share" stage, the instructor asks different follow-up questions that the students may not have considered, and even asks other roles questions about what they would do in response to decisions or actions of the group that is sharing. For example, the instructor may ask the hackers or the data brokers to discuss how they would react to responses to questions by the company.

The duration of this exercise in a class of 30 students was a total of 60 minutes, after distribution of the case study. The students were given background information (using the slides in Appendix A) by the instructor for 5 minutes, 5 minutes to read the case study, and then 5 more minutes to ask questions. Students were grouped into 5 groups of 6 students each and randomly assigned stakeholder roles.

Under the Think-Pair-Share strategy, students were allocated 5 minutes for individual thinking, where they were asked to come up with/write down at least 2 distinct points from the perspective of their assigned stakeholder. After that, the stakeholder groups were allocated 10 minutes to Pair, where the group assigned a recorder for the group, each group member was given 1.5 minutes to discuss their individual points, and the group reconciled the points to create group answers. Finally, at the Share stage, each group reporter was

given 2 minutes to share their answers. No particular emphasis was laid on the order of the groups during the share stage, but in both instances of the class exercise, either the customers or the Insurance company started sharing first. After the completion of this exercise, a survey was handed to the students that recorded the efficacy of the role-playing scenario case study. The time allocated for the survey was 20 minutes, making the total time for this class exercise 60 minutes.

4.3 Evaluating Student Work

While we did not directly assess the students in the pre-tests, we created rubric criteria for the activity that align with the learning outcomes (see Table 1). To evaluate the students using this rubric, instructors can follow up the activity with some open-ended questions as an assignment or part of an exam.

Learning Objective	Needs Improvement	Meets Expectations	Exceeds Expectations
Students will be able to distinguish between various actors threatening or safeguarding their personal data.	Students distinguish between only the consumer and the company.	Students distinguish between 3 to 5 actors of the actors discussed in class.	Students distinguish between the 5 actors discussed in class and add at least one additional actor that was not discussed in class.
Students will be able to critically analyze the ethical implications of personal data sharing.	Students do not differentiate between the good and the bad aspects of personal data sharing.	Students differentiate between the good and the bad aspects of personal data sharing, but do not explain the implications.	Students differentiate between the good and the bad aspects of personal data sharing and explain the implications.
Students will be able to communicate concerns related to sharing personal data.	Students do not express concerns in a meaningful manner.	Students express concerns in a meaningful but non-persuasive manner.	Students express concerns in a meaningful and persuasive manner.

Table 1. Proposed Rubric Criteria for Assessment

5. PROPOSED SOLUTIONS

Proposed solutions to the questions assigned to each role are as follows.

5.1 Setomo Insurance

Prompt: As a member of the IT strategy team, how might Setomo Insurance use the data collected by the DriveCool program? Who in the company should have access to this data?

Proposed Solution: The data collected by the company can be strategically utilized to enhance business operations and decision-making. Specifically, the company can assess the risk profile of individual drivers or groups of drivers within and between specific ZIP codes. For example, insurance companies might be interested in assessing the risk profile for teenage male drivers within and between two ZIP codes in TN. This can enable more accurate underwriting and pricing models. The data can also be used to identify safe drivers, offering opportunities for incentive programs or premium discounts. Additionally, analyzing driving patterns may help point out potentially fraudulent claims, thereby reducing losses. Another potential use of the data is monetization through partnerships or sales to marketing firms seeking insights into consumer behavior.

To ensure data privacy and appropriate usage, access to driver data should be governed through role-based access controls. For instance, the legal team may need access for processing claims, the marketing team for setting personalized premiums, the data analytics team for modeling and insights, and the IT team for ensuring data security and protecting against breaches. Each role should have access only to the specific

data necessary to perform its function, in alignment with data governance and compliance requirements. For example, while the marketing team may need access to current pricing for a customer, they do not need access to previous claims. On the other hand, the legal team does not need access to pricing data, but they need access to claims history.

5.2 Customers

Prompt: As a Setomo Insurance customer, why would some customers not want Setomo Insurance to have access to their driving-related data? Are there any particular types of customers who would be especially vulnerable if Setomo Insurance had their data? Could Setomo Insurance use the driving-related data in a way that would not be in the customers' best interests? What would happen if Setomo Insurance experienced a breach of the driving-related data?

Proposed Solution: When implementing data-driven insurance models, it is important to recognize that customer attitudes toward data sharing can vary significantly. Some customers may be hesitant to share personal data with the insurance company, even if incentivized by reduced premiums. This reluctance may stem from concerns about potential data breaches or a lack of transparency regarding how their data will be used by the company. Conversely, other customers may be more open to sharing their data if they perceive clear economic benefits, such as lower premiums, and if the data usage contributes to improved, personalized insurance services.

Particular attention must be given to vulnerable populations such as elderly individuals and people with disabilities. These groups may face a higher risk of data misuse or may not fully understand the implications of data sharing. Without strong consent mechanisms and clear communication, there is a risk that their data could be used in unintended ways. To mitigate these risks, it is essential to establish transparent data usage policies, ensure informed consent, and implement strong data protection measures. Clear communication about how data is collected, used, stored, and protected can help build trust. Otherwise, companies can easily find loopholes to sell the sought-after customer data to other marketing and big tech at premium prices without the concerned individual's informed consent.

In the event of a data breach, the customers will lose their faith in Setomo Insurance. This event can potentially create irreversible damage to the company's reputation and affect its bottom line.

5.3 Hackers

Prompt: As a hacker, how could you gain access to the driving data collected by Setomo Insurance? Why might you want to access this data?

Proposed Solution: In the context of connected vehicle technologies and IoT-enabled insurance services, several security vulnerabilities must be proactively addressed. One notable threat is the risk of unauthorized access to Bluetooth-enabled IoT devices installed in vehicles. Malicious actors could exploit these devices to extract sensitive data, which may then be sold to competing insurance providers or third parties for profit. Another plausible attack vector is the execution of a man-in-the-middle (MITM) attack. This could be used to intercept data transmissions between the IoT device and the insurance company's servers, thereby exposing vulnerabilities in Setomo Insurance's data security infrastructure. Such incidents could not only compromise the confidentiality and integrity of customer data but also damage the company's reputation and regulatory standing.

From a hacker's perspective one reason to access this data is to achieve financial objectives. On the other hand, an ethical hacker could inform the company and its customers of the vulnerabilities the insurance company has in its data collection process.

To mitigate these risks, it is imperative that Setomo Insurance implements end-to-end encryption for data transmission, ensures robust device authentication mechanisms, and routinely audits and updates all connected systems. A comprehensive cybersecurity framework, including intrusion detection systems, network segmentation, and regular penetration testing, should be established as a standard operating procedure (SOP) to identify and address potential threats before they can be exploited.

5.4 Data Brokers

Prompt: As a third-party data broker company, what value lies in the driving-related data collected by Setomo Insurance? Who would be interested in purchasing such data?

Proposed Solution: The information-laden driving data of customers, when joined with other data sources about them, is a rich knowledge base of consumer behavior across different domains. The value proposition of this data is immense. First, the driving-related data can help discern the individual's risk tolerance, lifestyle, and driving habits. Secondly, the insight gathered from the location data can be used to build geographic maps valuable for location-based marketing, infrastructure planning, and traffic management. Third, historical driving behavior can help in building predictive models for accident probability, vehicle wear, and insurance fraud likelihood. Lastly, understanding commuting habits, like car usage frequency or type of car, can help in creating personalized marketing across verticals like car wash services, garages, etc.

This makes the data highly sought after by the data brokers or data aggregators who can sell it to potential buyers like other insurance companies, automobile manufacturers and dealerships, ad agencies, financial lenders, urban planners and transport authorities, Tech companies and app developers, and retail and fuel providers.

5.5 Regulators

Prompt: As regulators, what privacy protection laws and standards currently protect customer data? How are these laws and standards different in different circumstances? How can these laws and standards be improved?

Proposed Solution: There is a critical need for robust and forward-looking regulatory frameworks to protect individual privacy and ensure ethical data practices, especially in light of rapidly evolving data collection technologies used by insurance and technology companies. Existing regulations such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) provide benchmarks for establishing individuals' rights over their personal data, including the rights to access, consent, and deletion.

However, as new methods of data collection emerge, particularly through IoT devices, mobile applications, and connected services, regulations must evolve to stay ahead of potential privacy risks. Proactive legislation should not only keep pace with technological advancements but ideally anticipate future developments to mitigate risks before they arise.

In addition to legislative measures, regulatory bodies should play a role in promoting privacy awareness among the public in general. Educational campaigns, clear disclosure requirements, and user-friendly consent mechanisms can empower individuals to make informed choices about their data. By ensuring transparency and accountability, such measures can build public trust and create a more ethically aligned data economy.

6. EVIDENCE

We pre-tested the case in two different classes: a graduate cyber ethics class and an undergraduate database class. Student reactions to the teaching case and the issues involved were positive. As expected in a class discussion, responses were initially shallow repetitions of background facts from the perspective of the assigned roles. However, once several groups had responded, the opportunity to engage students in discussions of how one group reacts to the suggestions and perceptions of other groups allowed the discussion to deepen. As a whole, students had a positive reaction to Setomo's program, with some concerns and suggestions about how to ensure proper protection of the data to be shared. The impact of students' limited familiarity with some roles, such as data brokers and regulators, required more intentional facilitation by the instructors.

After completing the case activity, students completed a survey about the case adapted from questions in Fleischmann et al. (2011) and Blanken-Webb et al. (2018). No credit or other incentive was given for the case activity or for completing the survey questions at the end of the activity, aside from the general

participation requirement for the students in the graduate cyber ethics class. One student's data was removed because the values noted in the Likert questions were answered in the opposite direction from what was indicated by the open-ended questions, leading us to believe that the student may have thought the scale was in the reverse direction. The average scores from the Likert survey questions are summarized by class in Table 2.

Number	Question	Graduate Cyber Ethics (n=14)	Undergraduate Database (n=20)
1	This class exercise increased my awareness about ethical dilemmas regarding personal data.	4.21	4.25
2	This class exercise increased my awareness of my own ethical intuitions.	3.86	4.05
3	This class exercise increased my critical reasoning skills.	4.21	3.95
4	This class exercise increased my professional judgement of ethical issues.	4.00	4.00
5	This class exercise increased my collaborative problem-solving skills.	4.07	3.95
6	This class exercise facilitated a culture of dialogue.	4.29	4.00

Table 2. Average Scores of Student Perceptions From Likert Scale Survey Questions

We also asked some open-response questions adapted from Fleischmann et al. (2011). While we did not directly assess the students in the pre-tests, the open response questions roughly align with the learning objectives. Specifically, 1) the first two questions deal with distinguishing the ethical perspectives of different actors similar to LO1, 2) the next two questions deal with critical analysis of ethical concerns similar to LO2, and 3) the last two questions are related to improved communication skills similar to LO3.

Overall, student responses indicate that the students who participated had a wide variety of previous coursework and experiences related to data privacy ethics. In response to "What did you learn about data ethics during this class exercise?", some students indicated that they already knew many of the concepts that were covered. However, many students noted that they had a more holistic understanding of the different stakeholder roles. For example, one student responded, "The different stakeholders and their roles. I 'knew' the stakeholders before, but a clear and concrete list and thought-provoking questions allowed me to gain a deeper understanding that wasn't surface level knowledge." Another student responded, "As a consumer, companies are always collecting data about my personal information. I need to be more aware of who I am sharing my data with." Some students noted specifically that they had not considered the market for personal data and third-party data brokers. Students also learned more about companies collecting personal data, sometimes data that is not directly relevant to the service provided.

In response to "Please explain how the group interaction helped you learn about data ethics, if at all.", students indicated that they tended to enjoy hearing other students' perspectives and that hearing other perspectives was valuable. One student responded, "Group interaction and perspective sharing is always useful when learning about ethics. Differing perspectives, given proper consideration, help me critically examine my own opinions, either to change, expand, or reinforce them." Others indicated it helped to practice communication and collaboration skills. However, not all groups functioned well. Some group members did not contribute to the discussion. In reflection, we believe this may be attributed to the activity not being a graded activity in the class. Closer monitoring of the group discussions and including the activity in part of the course grade may help with this.

When asked, "What did you learn about the value of your privacy during this class exercise?", students concluded that companies value their data more than the students value their own data. One student responded, "I learned that it's important to value your privacy. Look into what companies are actually doing with your data instead of brushing it off." Further, several indicated they are more aware of the data privacy situation and may take steps to protect their privacy in the future.

We also asked, "What did you learn about other people's value of privacy during this class exercise?" Some students indicated that they feel other students do not value their privacy as much as they should. Other students indicated that the whole group valued their privacy equally. Some students noted that people do not realize they are providing personal data; "People value their privacy only when it's a tangible thing they can see being intruded. Not something digital."

In response to the question, "Does this class exercise prepare you to analyze ethical concerns about your personal data? Please explain.", students reported a heightened sense of the importance of personal data and mindfulness in data sharing. One student wrote, "Yes, I think it illustrates how important my information is, and I need to be careful who I am sharing it with even to get a discount."

Finally, we asked, "After this class exercise, do you think adopting mitigation techniques to safeguard your privacy from a data breach is beneficial? If so, why and how do you intend to do so?" While this exercise was not intended to be a practical exercise in personal data security, student feedback indicated that they were interested in taking measures to change their behavior. Some students indicated they needed to do more research to determine what steps to take, responding, "I think so. I don't know how to go about it, but I want to safeguard my data because I feel uncomfortable with my sensitive information being accessed." This exercise may open the door for an appropriate class to move into a hands-on activity with regards to personal data privacy.

The instructor's role in the exercise was extended beyond leading the discussion of the case and the feedback about the ethical implications. The instructor also noted suggestions based on the discussion that can be used to improve the case itself. During the administration of the exercise, the instructor observed that students struggled to understand the regulator's role and responsibilities. The students' suggestions tended to be more generic and less substantial. In future administrations, instructors could address this issue by focusing on the role of regulators in legislating and enforcing privacy and security policies and laws when providing background to the students.

7. FUTURE EXPANSION OF THE CASE

The case is designed to be easily modifiable to a wide range of classes. While the instructor is the domain expert for any given class, we suggest some of the following ways that the case can be expanded. Most students will have little experience with laws related to data privacy so only a brief, high-level introduction was presented. However, a business law class could expand the case by adding references to relevant case law and providing additional details on laws such as the following:

- GDPR (General Data Protection Regulation) in the EU
- FCRA (Fair Credit Reporting Act) in the US
- GLBA (Gramm-Leach-Bliley Act) in the US for financial institutions
- PIPEDA (Personal Information Protection and Electronic Documents Act) in Canada

A website development class can expand the case by tying the case to discussions of topics such as:

- Bot detection
- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
- Rate limiting
- Dynamic tokens

A database class can expand the case by relating the case to topics such as:

- Privacy by design

- At rest encryption
- SQL injection
- Audit logging
- Masking
- Role-based access control

As presented, the case demonstrates value as a standalone exercise that engages in a scenario familiar to students, provides ample perspectives from which the case can be viewed, and is brief enough to easily comprehend and recall details. However, an important strength of the case is that it is also open enough to support expansion into a wide array of individual topic specialties.

8. CONCLUSION

The importance of teaching ethics to IS students prompted the development of this case. The technique described relies on practices suggested by the literature through the use of a role-playing exercise as a means of deepening student engagement with the exercise. At the heart of the exercise is a case with which students can readily identify and to which they can apply their own experiences. The case supports multiple perspectives on sharing personal data and the security concerns associated with such sharing. Students engage as one of five possible stakeholders, which leads to robust discussion of the ethical implications of privacy and security concepts. Empirical results from the use of the case with this technique suggest that student learning about ethics is enhanced, and that the exercise resulted in deeper consideration of ethical consequences by students. Calls in the literature suggest that this addresses an important need in the IS curriculum. Further, the case is also easily expandable to a wide range of IS and business-related courses, making the contribution potentially further reaching.

9. REFERENCES

Accreditation Board for Engineering and Technology. (2025). *Criteria for Accrediting Computing Programs, 2025 – 2026.* https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2025-2026

AlDhaen, E. (2025). Promoting Ethical Integration through AACSB Accreditation of Business Schools: Insights from Gulf Cooperation Council (GCC) Region. *Journal of Applied Research in Higher Education*. Advance online publication. https://doi.org/10.1108/JARHE-12-2024-0714

Anderson, L. W., & Krathwohl, D. R. (Eds.). (2001). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. New York, NY: Addison Wesley Longman, Inc.

Avin, S., Gruetzemacher, R., & Fox, J. (2020). Exploring AI Futures Through Role Play. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (pp. 8-14). New York, NY: ACM. https://doi.org/10.1145/3375627.3375817

Barry, B. E., & Ohland, M. W. (2012). ABET Criterion 3.f: How Much Curriculum Content is Enough? *Science and Engineering Ethics*, 18, 369-392. https://doi.org/10.1007/s11948-011-9255-5

Bietz, M. J., Cheung, C., Rubanovich, C. K., Schairer, C., & Bloss, C. S. (2019). Privacy Perceptions and Norms in Youth and Adults. *Clinical Practice in Pediatric Psychology*, 7(1), 93-103. https://doi.org/10.1037/cpp0000270

Blanken-Webb, J., Palmer, I., Deshaies, S. E., Burbules, N. C., Campbell, R. H., & Bashir, M. (2018). A Case Study-Based Cybersecurity Ethics Curriculum. *2018 USENIX Workshop on Advances in Security Education, ASE 18*, Baltimore, MD: USENIX Association. https://www.usenix.org/system/files/conference/ase18/ase18-paper_blanken-webb.pdf

Blatner, A. (2009). *Role Playing in Education*. https://www.blatner.com/adam/pdntbk/rlplayedu.htm

Brown, N., Xie, B., Sarder, E., & Wiese, E. (2024). Teaching Ethics in Computing: A Systematic Literature Review of ACM Computer Science Education Publications. *ACM Transactions on Computing Education*, 24(1), Article 6. https://dl.acm.org/doi/10.1145/3634685

Cappel, J. J., & Schwager, P. H. (2002). Writing IS Teaching Cases: Guidelines for JISE Submission. *Journal of Information Systems Education*, 13(4), 287-294. https://jise.org/volume13/n4/JISEv13n4p287.pdf

CC2020 Task Force. (2020). *Computing Curricula 2020: Paradigms for Global Computing Education*. New York, NY: ACM. https://doi.org/10.1145/3467967

Farhoomand, A. (2004). Writing Teaching Cases: A Quick Reference Guide. *Communications of the Association for Information Systems*, 13, 103-107. https://doi.org/10.17705/1CAIS.01309

Fleischmann, K. R., Robbins, R. W., & Wallace, W. A. (2011). Information Ethics Education for a Multicultural World. *Journal of Information Systems Education*, 22(3), 191-202. https://jise.org/volume22/n3/JISEv22n3p191.html

Hanschke, V. A., Rees, D., Alanyali, M., Hopkinson, D., & Marshall, P. (2024). Data Ethics Emergency Drill: A Toolbox for Discussing Responsible AI for Industry Teams. *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1-17). New York, NY: ACM. https://dl.acm.org/doi/10.1145/3613904.3642402

Howes, E. V., & Cruz, B. C. (2009). Role-Playing in Science Education: An Effective Strategy for Developing Multiple Perspectives. *Journal of Elementary Science Education*, 21(3), 33-46. https://link.springer.com/article/10.1007/BF03174721

International Organization for Standardization. (2024). *ISO/IEC 29100:2024 Information Technology — Security Techniques — Privacy Framework*. https://www.iso.org/standard/85938.html

Kaddoura, M. (2013). Think Pair Share: A Teaching Learning Strategy to Enhance Students' Critical Thinking. *Educational Research Quarterly*, 36(4), 3-24. https://eric.ed.gov/?id=EJ1061947

Maier, H. W. (2002). *Role Playing: Structures and Educational Objectives*. CYC-Online. https://www.cyc-net.org/cyc-online/cycol-0102-roleplay.html

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. *European Journal of Information Systems*, 18(2), 126-139. https://doi.org/10.1057/ejis.2009.10

National Institute of Standards and Technology. (2024). *Privacy Framework*. https://www.nist.gov/privacy-framework/privacy-framework

Shapiro, B. R., Lovegall, E., Meng, A., Borenstein, J., & Zegura, E. (2021). Using Role-Play to Scale the Integration of Ethics Across the Computer Science Curriculum. *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education* (pp. 1034-1040). New York, NY: ACM. https://dl.acm.org/doi/10.1145/3408877.3432525

Siponen, M. (2001). On the Role of Human Morality in Information System Security: From the Problems of Descriptivism to Non-Descriptive Foundations. *Information Resources Management Journal*, 14(4), 15-23. https://doi.org/10.4018/irmj.2001100102

Skirpan, M., Beard, N., Bhaduri, S., Fiesler, C., & Yeh, T. (2018). Ethics Education in Context: A Case Study of Novel Ethics Activities for the CS Classroom. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 940-945). New York, NY: ACM. https://dl.acm.org/doi/10.1145/3159450.3159573

Sogunro, O. A. (2004). Efficacy of Role-Playing Pedagogy in Training Leaders: Some Reflections. *Journal of Management Development*, 23(4), 355-371. https://doi.org/10.1108/02621710410529802

Widyasari, P. A. (2020). Roleplay "Conflict of Interest and Common Good": Business Ethic Teaching Method for Future Leader. *Advances in Natural and Applied Sciences*, 14(1), 160-167. http://www.aensiweb.net/AENSIWEB/anas/anas/2020/January/160-167(22).pdf

AUTHOR BIOGRAPHIES

Soham Sengupta is an Assistant Professor of Information Systems & Analytics in the Jones College of Business at Middle Tennessee State University in Murfreesboro, TN. He earned his Ph.D. in Management Information Systems from the University of Memphis in 2023. Dr. Sengupta currently teaches Management of Security Operations, Cybersecurity Ethics at the graduate level and Introduction to Microcomputing at the undergraduate level. His research interests include privacy, cyber ethics and top management team. He has presented his research at the Southeast Decision Sciences Institute. His published work has appeared in journals like the *Journal of Cancer Education* and *International Journal of Information and Operations Management Education*.

Stephanie A. Totty is an Assistant Professor of Information Systems & Analytics in the Jones College of Business at Middle Tennessee State University in Murfreesboro, TN. She earned her Ph.D. in Management Information Systems from the University of Memphis in 2022. Dr. Totty currently teaches Applied Business Analytics, Big Data for Analytics, and Data Mining and Predictive Analytics at the graduate level. Her research interests include security and software development teams. She has presented her research at the *Americas Conference on Information Systems*. Her published work has appeared in journals including *Communications of the Association for Information Systems*, *The Data Base for Advances in Information Systems*, the *Journal of Information Systems Applied Research*, the *Journal of Organizational and End User Computing*, and the *Journal of Information Technology Management*.

Steven A. Morris earned the Ph.D. in Management Information Systems from Auburn University. He is a Professor in the Information Systems and Analytics Department in the Jones College of Business at Middle Tennessee State University. He primarily teaches classes in Database Design and Development, and Advanced Database Programming. Dr. Morris actively consults with businesses in the Middle Tennessee area on database-related projects. He has published dozens of articles in scholarly journals on diverse topics including databases, project management, virtual teams, and pedagogical issues. He is also the co-author of *Database Systems: Design, Implementation, and Management*, a textbook that is currently in its 14th edition**.**

APPENDICES

Appendix A. Background Slides

What is security?

The act of protecting data from unauthorized access & cyber threats.

Key Risks: Data leaks, identity theft, cyberattacks.

Infosec Strategy	Description
Data Encryption	Secures sensitive data during storage and transmission.
Access Controls & Permissions	Restricts data access based on user roles.
Secure Data Storage	Ensures protection against unauthorized access and breaches.
Employee Training & Awareness	Reduces human-related security risks.
Incident Response & Management	Enables swift action in case of security breaches.
Regular Software Updates & Patches	Addresses vulnerabilities to prevent exploits.

What is privacy?
Privacy is an individual's fundamental right to be left alone without interference or intrusion. It is the ability and choice of an individual to keep their personal information and life private and free from intrusion and manipulation.

Why is it important to safeguard our personal information?
In today's digital age, it is pivotal to safeguard the online personal information of an individual to prevent identity theft and various forms of social engineering hacks that individuals are subjected to after sharing their personal information online.

Why would someone provide private information to a company?
One would provide personal information to companies in anticipation of getting better services and products through reduced pricing, loyalty programs, and others.

Why would a company be interested in collecting private information?
In today's data economy, data is the new gold. Detailed information about consumers as much as possible gives companies the edge to provide the best services and products. Sell the collected data for additional revenue to marketing firms and other companies willing to pay for advertising.

What data is considered private?
Any data that can be used to identify an individual can be considered private data. Examples are

- Health data.
- Work-related.
- DOB.
- Location data.

Why do businesses secure data?
Data security is pivotal for a company's reputation, as data breaches can lead to diminishing brand value and loss of trust from existing and prospective customers and shareholders.

How do businesses use our data?
Businesses use our data to provide customized services, offers, and products. They constantly train their machine learning models with the customer's data to create more value in their services and products that surpass their competitors.

Are businesses using our data for the reason we provide data in the first place?
Personal data about consumers is such a prized entity in today's data economy that there is a huge appetite for hoarding data by companies and data aggregators (aka data brokers). This opportunity, clubbed with loose data regulations, allows businesses to use/ sell personal data for other purposes.

What kind of strategies do companies adopt to safeguard personal information?

- **Privacy by Design** - Companies adopt a strategy of proactively incorporating privacy as a core requirement during the design and development of services and products. This helps in ensuring maximum data privacy for customers as a default setting.
- **Cookie Preferences/ Consent** - Companies can remove unwarranted third-party data brokers scraping data from across the web using APIs and other means.
- **Privacy Policies** - Companies can update their privacy policies to maintain compliance with privacy regulations and provide visibility and transparency about their customers' data collection and storage.

Who are the stakeholders?

- **Company** – The insurance company that is providing the service in exchange for collecting driving information of customers and complying with data privacy.
- **Customers** – The service beneficiary whose data is being obtained.
- **Hackers** - anonymous entities (individuals or groups) that aim to obtain illegal access to electronic data, networks, and systems of desirable targets, mainly to achieve financial gain.
- **Third-party data brokers** - Data brokers are data aggregators that collect data from various sources and aggregate it to build individual profiles and sell it to marketing companies.
- **Regulators** - Regulators are the gatekeepers who develop and enforce privacy-protecting rules. Any failure to do so will give the regulators the right to showcase the companies and revoke the data broker's license. The regulator's objective is to safeguard the consumer's data from being exploited by companies and other entities.

Appendix B. Scenario

Setomo Insurance, an auto insurance company, has launched a new program called DriveCool to better serve its customers. Customers who enroll in the DriveCool will receive discounted insurance rates. For example, one customer received a $150 discount on a 6-month contract that was already market-appropriate.

After enrolling in the DriveCool program, the user installs an app on their phone and a company-provided Bluetooth-enabled IoT device in their vehicle. The IoT device must always be paired with the user's phone to obtain and report the driving-related data to the company. If the location sharing or Bluetooth is disabled at any time, the app will send numerous notifications to reenable location sharing or Bluetooth, respectively. Setomo Insurance may unenroll the user from the DriveCool program if the user disables location sharing or Bluetooth, disallowing them to enjoy the competitive rates.

The discount is very desirable for customers, but customers must provide the company with some of their personal information to receive the benefit.

Appendix C. Role Cards

Role: Setomo Insurance

The insurance company that is providing the service in exchange for collecting driving information of customers and complying with data privacy.

As a member of the IT strategy team at Setomo Insurance,

- How might Setomo Insurance use the data collected by the DriveCool program?
- Who in the company should have access to this data?

Role: Customer

The service beneficiary whose data is being obtained.

As a Setomo Insurance customer,

- Why would some customers not want Setomo Insurance to have access to their driving-related data?
- Are there any particular types of customers who would be especially vulnerable if Setomo Insurance company had their data?
- Could Setomo Insurance use the driving-related data in a way that would not be in the customers' best interests?
- What would happen if Setomo Insurance experienced a breach of the driving-related data?

Role: Hacker

Anonymous entities (individuals or groups) that aim to obtain illegal access to electronic data, networks, and systems of desirable targets, mainly to achieve financial gain

As a hacker,

- How could you gain access to the driving data collected by Setomo Insurance?
- Why might you want to access this data?

Role: Data Brokers

Data brokers are data aggregators that collect data from various sources and aggregate it to build individual profiles and sell it to marketing companies.

As a data broker company,

- What value lies in the driving-related data collected by Setomo Insurance?
- Who would be interested in purchasing such data?

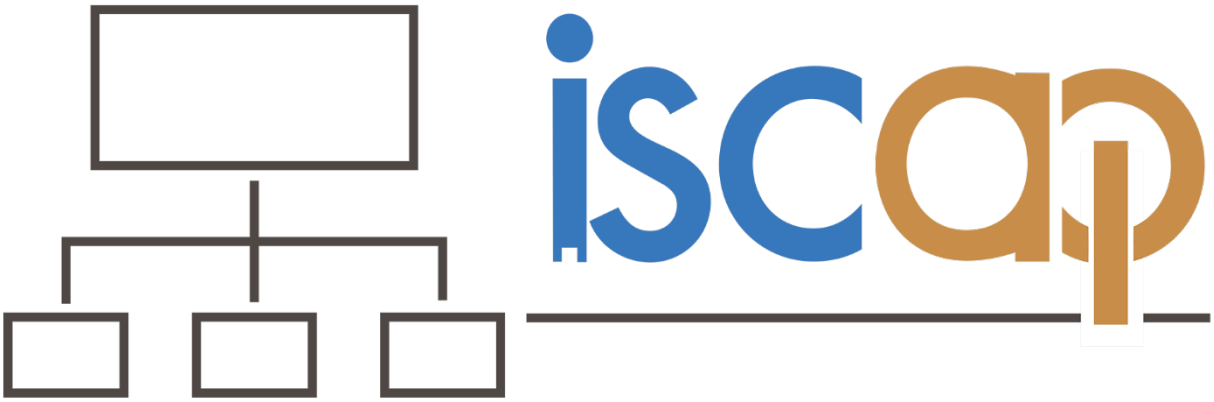
Role: Regulator

Regulators are the gatekeepers who develop and enforce privacy-protecting rules. Any failure to do so will give the regulators the right to penalize the companies and revoke the data broker's license. The regulator's objective is to safeguard the consumer's data from being exploited by companies and other entities.

As regulators,

- What privacy protection laws and standards currently protect customer data?
- How are these laws and standards different in different circumstances?
- How can these laws and standards be improved?

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)