Computational Thinking Module

Your Data and Your Privacy:
Do you know what “they” can tell about you?

STUDENT EDITION
VCTAL

The Value of Computational Thinking Across Grade Levels

Computational Thinking Module

Your Data and Your Privacy:
Do you know what “they” can tell about you?

STUDENT EDITION

By

Paul Kehle
Rebecca Wright
Your Data and Your Privacy:
Do you know what “they” can tell about you?

What Is Computational Thinking?
Computational thinking is a high-level thought process that considers the world in computational terms. It begins with learning to see opportunities to compute something, and it develops to include such considerations as computational complexity; utility of approximate solutions; computational resource implications of different algorithms; selection of appropriate data structures; and ease of coding, maintaining, and using the resulting program. Computational thinking is applicable across disciplinary domains because it takes place at a level of abstraction where similarities and differences can be seen in terms of the computational strategies available. A person skilled in computational thinking is able to harness the power of computing to gain insights. At its best, computational thinking is multidisciplinary and cross-disciplinary thinking with an emphasis on the benefits of computational strategies to augment human insights. Computational thinking is a way of looking at the world in terms of how information can be generated, related, analyzed, represented, and shared.

Introduction to the Module
This module introduces students to privacy issues that are created, worsened, or solved by computer technology and the collection of data. The module is driven by a series of case studies drawn from various well-known websites. It also examines a surprising way in which a computational strategy can protect privacy. The concluding activity has students create a proposal for the design of a Compute-a-Date dance website; in their proposal, the students are expected to apply what they've learned about privacy issues through the case studies in this module.

The focus of the module is on how our ideas about privacy and personal conduct need to change in response to evolving technologies and the proliferation of data-collection tactics. Often there are no clear answers to questions about privacy, as evidenced by numerous court cases. When answers are not clear, the focus should be on becoming more informed and holding careful and informed discussions.
<table>
<thead>
<tr>
<th>is an author</th>
<th>has a daughter named Jessica</th>
</tr>
</thead>
<tbody>
<tr>
<td>is from England</td>
<td>has one sister</td>
</tr>
<tr>
<td>born on July 31st</td>
<td>born in 1965</td>
</tr>
<tr>
<td>likes the band “The Smiths”</td>
<td>is a billionaire</td>
</tr>
<tr>
<td>remarried and had a son and a daughter</td>
<td>once ranked 2nd-richest female entertainer in the world</td>
</tr>
<tr>
<td>lived on welfare</td>
<td>has assisted in writing film scripts</td>
</tr>
<tr>
<td>is a woman</td>
<td>mother died of multiple sclerosis</td>
</tr>
<tr>
<td>was given no middle name</td>
<td>worked with director Chris Columbus</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>is a famous Leo</td>
<td>the idea for a novel came while on a train ride</td>
</tr>
<tr>
<td>has been published</td>
<td>had several books listed on the <em>New York Times</em> best-seller list</td>
</tr>
<tr>
<td>is president of a charity</td>
<td>several movies have been based on this person's books</td>
</tr>
<tr>
<td>when 6 years old, wrote a book about a rabbit</td>
<td>owns 3 houses</td>
</tr>
<tr>
<td>was divorced</td>
<td>inspired the character Hermione Granger</td>
</tr>
<tr>
<td>knows a lot about Azkaban</td>
<td>was told by her editor to create a middle name</td>
</tr>
<tr>
<td>born on January 29th</td>
<td>is a woman</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>was a news anchor</td>
<td>born in 1954</td>
</tr>
<tr>
<td>coauthored at least five books</td>
<td>interviewed Michael Jackson</td>
</tr>
<tr>
<td>was in a Steven Spielberg film</td>
<td>is black</td>
</tr>
<tr>
<td>learned to read before age 3</td>
<td>runs an educational charity</td>
</tr>
<tr>
<td>is a philanthropist</td>
<td>born in Mississippi</td>
</tr>
<tr>
<td>started a school in Africa</td>
<td>promotes books</td>
</tr>
</tbody>
</table>
### Master #2 for Pooling Information Activity (Sheet 2 of 2)

<table>
<thead>
<tr>
<th>has her own website</th>
<th>received a full scholarship to Tennessee State University</th>
</tr>
</thead>
<tbody>
<tr>
<td>raised by grandmother for first 6 years of life</td>
<td>grew up in a very poor family</td>
</tr>
<tr>
<td>involved in more than 5 movies</td>
<td>loves dogs</td>
</tr>
<tr>
<td>only child died at very early age</td>
<td>founded a leadership academy for girls</td>
</tr>
<tr>
<td>introduced Dr. Phil to America</td>
<td>views Maya Angelou as mentor</td>
</tr>
<tr>
<td>richest woman in entertainment</td>
<td>published two magazines</td>
</tr>
<tr>
<td>hosted a morning talk show</td>
<td>first black female billionaire in the United States</td>
</tr>
</tbody>
</table>
Homework: Assembling Clues to a Mystery Person
Choose a fairly well-known person and research him or her on the Internet. Choose ten facts about this person to present as clues for your classmates to use in trying to guess who your mystery person is. Order the clues from 1 to 10 in increasing order of specificity. Begin with clues that apply to a large number of people. End with clues that are very specific or unique to your mystery person. Order the clues so that your classmates become increasingly confident but are not 100 percent sure until you tell them the tenth clue. No two clues, including the ninth and tenth clues, should be enough by themselves to reveal the identity of your mystery person.
Clues:
1. 
2. 
3. 
4. 
5. 
6. 
7. 
8. 
9. 
10. 
Unit 2: Case Studies in Privacy

Objective: Students will be able to identify, analyze, and explain privacy issues that can arise in a variety of situations.
Case Study #1

Name: __________________________

Netflix: Who’s Watching What You Watch?

The Scenario
Netflix is an American company providing on-demand Internet streaming movies and TV shows and a flat rate DVD-by-mail service with no deadlines, for as little as $8 a month (in 2012). Netflix also offers its customers movie recommendations based on their viewing history and on how they’ve rated what they’ve watched. When creating a Netflix account, a customer provides a credit-card number and personal information that includes, among other data, a name, an address, an age, and preferred categories of movies. Customers must trust Netflix to keep their personal information safe from others. When a customer cancels a Netflix membership, all the personal information, including the rental history, should be deleted.

Initial Prompts
How could Netflix and its services involve issues of privacy?
How could Netflix take advantage of its customers’ information?
How could someone else take advantage of the information Netflix collects?

Additional Details
Netflix held a contest in 2006, challenging computer scientists to create a better movie-recommendation algorithm. The reward would pay $1 million to the first person or team of people to make significant improvements to its recommendation system. The contest was very popular and the company sent more than 50,000 contestants large amounts of data. The data included 100 million movie ratings and the date of each rating all correlated with unique ID numbers in place of customers’ names. To be clear, no customer names were included in the data.

Perfectly reasonable—right? What could go wrong?
Case-Study Privacy Questions

1. What private information is collected and how is it collected?

2. Could someone’s privacy be violated? Why and how, or why not?

3. Who could benefit from sharing the private information or from combining it with information from other sources? Would such acts be justifiable?

4. How could privacy violations be prevented in this situation? Are there technological strategies for better protecting privacy?

5. What are the pros, cons, and compromises resulting from the sharing of private information in this situation?

6. How has this case study affected your thinking about privacy?
Case Study #2

Facebook’s Missing Beacon

The Scenario
Surely you've heard of Facebook. Back in 2009, there were about 300 million users, three years later that figure had doubled. Much has changed and much is still changing with how this site operates; however, one thing has always been true, Facebook is all about information—your information. Even if your online friends and cyber strangers may not be able to see some of the information you share, it’s still all there, just waiting to be connected with other information. In 2007, Facebook thought it would be great to link people’s activities on other websites to their Facebook accounts.

Initial Prompts
How could Facebook and its services involve issues of privacy?
How could Facebook take advantage of its users’ information?
How could someone else take advantage of the information Facebook collects?

Additional Details
Turn back the clock to 2009 and imagine you had just gone onto the ticket-selling website Fandango to purchase tickets to see *Harry Potter and the Half Blood Prince*, against your mother’s wishes. She doesn’t understand and feels it is a bad influence on you. You consider not buying them, but you love Harry Potter and it means a lot to you to go with your friends, so you click the purchase button. As soon as you hit that button, “Alex Brown purchased tickets for *Harry Potter and the Half Blood Prince* at Fandango.com” is posted on your Facebook profile, and appears on your friends’ news feeds. Unfortunately, you are Facebook friends with your aunt, who sees your recent purchase in her news feed. She immediately calls your mom, and the next thing you know, your mother is demanding that you give her the tickets, and now you are no longer able to go to see Harry Potter.
Case Study #2

The above scenario was made possible by a program called Beacon.

As part of an advertising scheme, Facebook installed Beacon on November 6, 2007. Beacon was a program that allowed Facebook to partner with many other websites, including, eBay, Fandango, Zappos.com, Yelp, National Basketball Association, and Sony Online Entertainment LLC. The partnering allowed a user's non-Facebook activity to be recorded and then posted to his or her Facebook friends through the news feed. When a user is logged into a Facebook session and browsing a partner site, through Beacon the partner site reports behavioral events concerning the user’s actions to Facebook. Behavioral events include tracking a consumer’s web activities (e.g., searches conducted, web pages visited), and knowing consumers’ behavioral events helps companies deliver advertising targeted to an individual consumer's interests. Through Beacon, Facebook was able to produce targeted advertising for each individual user. Although an opt-out option was available, it was not always clearly indicated, and it was an issue because users had to opt-out on each site visited; you could not turn the system off globally. At one point, some critics claimed that even if you opted out, Facebook was still sent the behavioral data.
Case-Study Privacy Questions

1. What private information is collected and how is it collected?

2. Could someone’s privacy be violated? Why and how, or why not?

3. Who could benefit from sharing the private information or from combining it with information from other sources? Would such acts be justifiable?

4. How could privacy violations be prevented in this situation? Are there technological strategies for better protecting privacy?

5. What are the pros, cons, and compromises resulting from the sharing of private information in this situation?

6. How has this case study affected your thinking about privacy?
Case Study #3

23andMe and You and You?!

The Scenario
In the privacy of your own home, through the website www.23andme.com, you are now able to have your DNA analyzed and learn about your personal genomics for only $99. You mail in some saliva and about 6 weeks later you receive data that identifies not only your risk of developing more than 190 genetic diseases but also aspects of your ancestry.

Initial Prompts
Did you know that this type of service was possible?
How could 23andMe involve issues of privacy?
How could 23andMe take advantage of its customers’ information?
How could someone else take advantage of the information 23andMe collects?

Additional Details
Heidi came across the website 23andme.com when randomly searching online. She was curious and discovered that she can mail the company some spit and learn about her DNA sequence, which can reveal what diseases she is likely to get as well as information about her ancestry. “Cool!” Heidi thought. Six weeks later, the results came, confirming a lot of what Heidi already knew, such as her physical traits, including her blue eyes and straight hair. But then she discovered that she has an elevated risk for Alzheimer’s disease. The average risk is 7.2 percent, while hers is 18 percent. She is over two times more likely to contract the disease than the average person is. But then Heidi gasped. The data revealed that her mother’s side of the family originated in Scandinavian populations. But her mother is clearly Irish, which is what Heidi thought she was. As Heidi continued reading, she saw a section for “Your Family and Friends.” In this section was a small list of people in her ancestry group who had also had their genomes analyzed and one of them, with an unfamiliar name, was listed as her mother! After her initial shock, Heidi called her father who after some coaxing and a guilty pause said, “Yes, Heidi, you were adopted.”
Case-Study Privacy Questions

1. What private information is collected and how is it collected?

2. Could someone's privacy be violated? Why and how, or why not?

3. Who could benefit from sharing the private information or from combining it with information from other sources? Would such acts be justifiable?

4. How could privacy violations be prevented in this situation? Are there technological strategies for better protecting privacy?

5. What are the pros, cons, and compromises resulting from the sharing of private information in this situation?

6. How has this case study affected your thinking about privacy?
Case Study #4

Google Auto Complete: Did you mean Google autocomplete?

The Scenario
Autocomplete is a feature of many word processors and websites that automatically completes and, in some cases, corrects a word or phrase that you have just begun to type. When typing a word into the Google search window, the autocomplete feature immediately produces a number of the most-popular searches based on what you have typed so far. As you continue to type, the list is instantly updated to match what you have typed. It is advertised as a handy time-saving feature.

Initial Prompts
What are the benefits of Google autocomplete?
How could Google autocomplete involve issues of privacy?

Additional Details
Imagine having a school project on the U.S. presidents. Unfortunately, you do not remember how to spell some of the names. You start to type in Rutherford Hayes, and Google’s autocomplete quickly produces the full name even though you've only entered part of it. Problem solved. Or maybe you typed the whole name and left out an e. Google will automatically catch your mistake and ask if you meant something else, all based on the most-popular searches that most closely resemble yours.

Google Instant, the computer program that makes autocomplete possible, was introduced in the United States on September 8, 2010. Google expects autocomplete to save users several seconds in every search. Google’s website explains: “As you type, Google's algorithm predicts and displays search queries based on other users’ search activities. If you're signed in to your Google Account and have Web History enabled, you might also see search queries from relevant searches that you've done in the past. . . . all of the predicted queries that are shown in the drop-down list have been typed previously by Google users.”
Case Study #4

Now imagine typing your own name into Google only to see that autocomplete follows your name with words like “criminal” or “conspiracy” or “dangerous”? Of course you are none of these things, but perhaps someone with a name very similar to yours is in the news and people have been searching for information. Note that it doesn’t matter whether other people’s searches are accurate. One misspelling in the public media is all it would take for your name and identity to be confused with someone else’s identity.

A man in Italy faced this sort of problem in April 2011. When searching his name on Google, two results came up: truffatore (con man) and truffa (fraud). What would you do in this situation? This man sued Google, and he won.

What other problems can you imagine resulting from using Google autocomplete?

Note that there is a difference between auto corrections of spelling errors and auto completions of partially entered search terms. Both features can lead to unexpected results.
Case-Study Privacy Questions

1. What private information is collected and how is it collected?

2. Could someone's privacy be violated? Why and how, or why not?

3. Who could benefit from sharing the private information or from combining it with information from other sources? Would such acts be justifiable?

4. How could privacy violations be prevented in this situation? Are there technological strategies for better protecting privacy?

5. What are the pros, cons, and compromises resulting from the sharing of private information in this situation?

6. How has this case study affected your thinking about privacy?
Case Study #5

Are Loyalty Cards Loyal to You?

The Scenario
In the checkout line at many stores, cashiers ask customers for their loyalty cards, membership cards, or frequent-shopper cards, or if they would like to sign up for some sort of membership or loyalty card. At many stores, you have to scan your card or else risk delaying the checkout process. These cards, similar in size to credit cards, can provide the shopper with discounts and special privileges available only to cardholders.

Initial Prompts
What are the benefits of loyalty cards?
How could loyalty cards involve issues of privacy?

Additional Details
A woman and her husband have just found out that they will be having a baby. As is common, they want to wait to announce the pregnancy until it is much further along, especially since no one knows they were thinking about starting a family. Their doctor has recommended some prenatal vitamins available at a local pharmacy, and the couple has begun to read up on what to expect during pregnancy.

A week later, the woman’s mother drops by for a visit and, as she often does, she brings in the mail. She is somewhat surprised to see a large flyer for baby diapers but figures it’s a random coupon. Then she notices more coupons, for Newborns R Us, for baby strollers, for baby food, for Paint Colors of Celebrities’ Nurseries, and a complimentary issue of New Parent Digest. “What’s going on here?” she thinks.

She opens the door with a big smile on her face, “Anything you want to tell me?” Her daughter spots the coupons, blushes, and quickly says, “We must have gotten on some mailing list by mistake.” But her mother is not convinced...
Case-Study Privacy Questions

1. What private information is collected and how is it collected?

2. Could someone’s privacy be violated? Why and how, or why not?

3. Who could benefit from sharing the private information or from combining it with information from other sources? Would such acts be justifiable?

4. How could privacy violations be prevented in this situation? Are there technological strategies for better protecting privacy?

5. What are the pros, cons, and compromises resulting from the sharing of private information in this situation?

6. How has this case study affected your thinking about privacy?
Should Foursquare Know Where You Aren’t?

The Scenario
Foursquare is similar to Twitter and other social-networking sites, except that Foursquare is based on location-specific posts. (The Gowalla and MyTown sites are two other examples.) Individuals log on from either a computer or a mobile device and as they update their location and activities, they can receive information about the places that are near them. Foursquare location posts are visible to all members, unless users change their settings to “Off the Grid” mode.

Initial Prompts
What are the benefits of location-specific web-information services?
How could a web service like Foursquare involve issues of privacy?

Additional Details
The Taylor family was very excited. They had just won a popular Family Night Out contest sponsored by a local business. The evening included dinner, a movie, and dessert afterward, all at the favorite places of the family and all paid for by the radio station. The family rarely all went out together because of their busy schedules; however, this opportunity was too good to pass up. The family members immediately broadcast their luck on their social-networking sites.

On the big night, as they were on their way to dinner, the son posted their plans on Facebook. His mother sent tweets to all her coworkers, and her daughter posted regular updates to Foursquare as the evening progressed. Foursquare was very helpful as it contained information on cool shops near the movie theater, so they got some shopping in also. They had a wonderful evening and arrived home quite late to find that their house had been robbed!
Case-Study Privacy Questions

1. What private information is collected and how is it collected?

2. Could someone’s privacy be violated? Why and how, or why not?

3. Who could benefit from sharing the private information or from combining it with information from other sources? Would such acts be justifiable?

4. How could privacy violations be prevented in this situation? Are there technological strategies for better protecting privacy?

5. What are the pros, cons, and compromises resulting from the sharing of private information in this situation?

6. How has this case study affected your thinking about privacy?
Unit 3: Computing to the Rescue: What’s our average?

*Objective:* Students will be able to explain what Secure Multiparty Computation (SMC) is in general and will be able to use an SMC algorithm to calculate the average of a group of numbers.
Secure Computing Activity

Name:_______________________________

The Problem
Suppose a group of five farmers wants to know how many total tons of beets they have produced but do not want to reveal how much any individual farmer has produced. If they can calculate the average of their five values, then they could multiply the average by five and know the total.

The Simulation
You will be one of five farmers (A through E) in a group and will receive a card with your value, the number of tons of beets you produced. Do not share your value with any other farmer. Next, you and the farmers in your group will follow an algorithm for Secure Multiparty Computation. You will each follow the same general steps; however, each of you will be working with your personal number.

The Algorithm
1. In the table that follows, enter your value on the “actual value” row under the corresponding farmer’s label.
2. Divide your value by 5 (because there are five farmers) and round to the nearest integer; enter the result in the corresponding “one fifth of value” row.
3. Choose four random integers, such that each one is greater than or equal to 0 and less than 100. Enter them under your column in the four boxes provided.
4. Find the sum of your four random numbers and enter it in your column on the row labeled “sum of #1 thru #4. Leave the row labeled “calculated #5” blank for now.
5. Round your sum up to the nearest 100. For example if the sum of your four random numbers is 124, then rounding up gives you 200, or if your sum is 87, then rounding up gives you 100, or if your sum is 300, then rounding gives you 300. Enter the rounded-up value in your column on the row labeled “round sum up to nearest multiple of 100”.
6. Now you will determine what your “calculated #5” value is. Add your “one fifth of value” to your “rounded sum” and then subtract your “sum of #1 thru #4.” Enter the result both in the row labeled “(one fifth value) + (rounded sum) – sum,” and in the row labeled “calculated #5.”
Secure Computing Activity

7. Share everyone’s five random numbers. Now Farmer A (and only Farmer A) is given everyone’s “random #1” number. Farmer B is given everyone's “random #2” number, Farmer C is given everyone’s “random #3” number, and so on. Each farmer receives four random numbers, one each from the other four farmers. After all the numbers have been distributed and recorded by the appropriate farmer, each farmer will focus on one corresponding row of random numbers. Farmer A will work with the five “random #1” numbers, Farmer B will work with the five “random #2” numbers, Farmer C will work with the five “random #3” numbers, and so on. Use sticky notes to share and track these numbers: From: Farmer A To: Farmer B Number: ___.

8. Each farmer now works with the corresponding row of random numbers. Each farmer sums the five random numbers, and divides the sum by 100, noting what the remainder is. (This operation is known as taking the MOD of a number. For example, 242 MOD 100 = 42, and 395 MOD 100 = 95, and 200 MOD 100 = 0, and 38 MOD 100 = 38, etc.) Enter the result of your MOD operation in the row just to the right of your five random numbers.

9. Now everyone can tell each other the result of their MOD calculations. As a group, find the sum of the five MOD numbers. Then find the MOD 100 of this sum. (Find the remainder after you divide the sum by 100.) Enter this remainder in the box provided. This number is the average of the five original values the farmers were given.

10. Finally, multiply this average by 5 to obtain the sum of the five farmers’ numbers. Check your results by showing each other your index cards and calculate the average and sum directly.

If your calculated average and sum differ from what you expected, carefully check your work. There are many steps to this algorithm and many places to make a small but significant mistake. In a true-life setting, a computer would be used to avoid making mistakes.
Secure Computing Activity

Use the table below to record the results of your computations.

<table>
<thead>
<tr>
<th>Five Farmers:</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>actual value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Average</td>
</tr>
<tr>
<td>one fifth of value</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Average</td>
</tr>
<tr>
<td>random #1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(sum #1's) MOD 100</td>
</tr>
<tr>
<td>random #2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(sum #2's) MOD 100</td>
</tr>
<tr>
<td>random #3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(sum #3's) MOD 100</td>
</tr>
<tr>
<td>random #4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(sum #4's) MOD 100</td>
</tr>
<tr>
<td>calculated #5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(sum #5's) MOD 100</td>
</tr>
<tr>
<td>sum of #1 thru #4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(sum MOD's) MOD 100</td>
</tr>
<tr>
<td>round sum up to nearest multiple of 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(one-fifth value) + (rounded sum) - sum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Discussion Questions

What do you think of this Secure Multiparty Computing algorithm?

Do you trust it to get the correct answer?

Do you trust it to protect the privacy of the individual values?

What are its strengths and weaknesses?
Unit 4: Designing a Computer Dating Website That Protects Privacy

(Concluding Assessment Project)

*Objective:* Students will be able to demonstrate and apply what they've learned about privacy to the design of a blind-dating website.
Concluding Privacy Project: Designing a Compute-a-Date Website

Think back over what you've learned about privacy in this module. You are now asked to apply what you've learned to a new situation. Some of the ideas you've encountered in the case studies will apply directly to the new situation. But some aspects of this new situation will require you to adapt or modify some ideas as you transfer them to the new situation. Often, the key to solving a new problem is seeing how to transfer ideas from familiar situations to a new situation. This transfer of understanding relies on general principles or a more abstract understanding of the specific examples you are familiar with. In brief, learning can be defined as coming to understand something new by adapting our understanding of what is already familiar to us.

Your Assignment
Students in a high-school student club and their faculty advisers want to create a Compute-a-Date website and have hired you as a Privacy Consultant. You need to help them think about the design of a computer system that would allow students to go to a website and be matched with another student for a blind date. Students would provide information to be used to match them for a blind-date dance party.

The system will enable students to enter some of their interests, characteristics, and preferences and then would provide a list of profiles (no names) of students who have entered similar information. The list of possible dates will be based on matching mutual interests and characteristics, but the list will not include names. If two students each approve the other’s profile, then they agree to be each other’s blind date. They will find out the identity of their dates at the dance. If no match is mutually approved, the students will not be matched.
Concluding Privacy Project: Designing a Compute-a-Date Website

Apply what you’ve learned in this module to the overall policies and parameters for a Compute-a-Date website. The system will collect information from students and match them for a blind-date dance. Students will get to know only certain pieces of information about their possible dates. You do not need to specify the details of how people will be matched. You do, however, need to explain how the interface will work. In particular, think about what information will be collected, how it will be collected, how it will be used, who will have access to it, how it will be shared, and how it will be discarded. Think about such things as defaults, opting in, opting out, degrees of public versus private sharing, and so on. Come up with a plan that you would recommend to the high-school class officers, and summarize any privacy-related issues you think they should pay close attention to.
Glossary

**algorithm**  An explicit method for solving a problem that has been proven to work.

**Computational thinking**

A way of looking at and thinking about the world in terms of how information and data can be defined, generated, collected, related, analyzed, represented, and shared using computers and other information technologies.

**default**  The way something is done in the absence of other preferences being provided.

**MOD**  Short for *modulus* or *modulo*; an operation in mathematics that gives the remainder when a whole number is divided by another whole number. For example, the result of $17 \text{ MOD } 12$ is $5$ because if we divide $17$ by $12$, the remainder is $5$. Similarly, $213 \text{ MOD } 100 = 13$; $400 \text{ MOD } 50 = 0$; and $199 \text{ MOD } 100 = 99$.

**opt-in**  A way of deciding whether a customer will have a service provided by a company in which the customer must explicitly indicate that he or she wants to have the service; the default is for the customer to not have the service.

**opt-out**  A way of deciding whether a customer will have a service provided by a company in which the customer must explicitly indicate that he or she does not want to have the service; the default is for the customer to have the service.

**parameter**  A value that can be adjusted to suit a particular purpose in a program or process. In most web browsers, the user can decide after how many days the web history of the browser will be cleared. This value can be changed, depending on the needs of the user; the value is a parameter associated with how the web browser functions.
**privacy**  A context in which a person controls who knows what about him or her and controls what someone else does with information that is shared. A private context is the opposite of a public context; in a public context, a person has very little control over who knows what or what others do with what they know.

**Secure Multiparty Computation**

A type of algorithm that allows a group of people to compute results based on individual values without the people needing to share their individual values.

**setting**  A value that can be adjusted to control how a program or process functions. When you determine when the screen saver will start on your computer by entering a particular number of minutes; you are selecting a setting. Similar to a parameter.