2014 CptS Professional Skills Discussion Assessment Report

Chris Hundhausen

Chair, CS & EECS Assessment Committee

1. Background

The Computer Science (CptS) at Washington State University's (WSU's) School of Electrical Engineering and Computer Science (EECS) has identified five student outcomes as being related to "professional skills." These outcomes, together with the associated performance indicators that have been established within the CptS program, are presented below:

D *An ability to function effectively on teams to accomplish a common goal*.

1. Fulfills different roles on teams and in meetings.
2. Fulfills individual responsibilities outside of team meetings.
3. Gives feedback; seeks and is receptive to feedback; seeks and appreciates different approaches or perspectives of other team members.

E *An understanding of professional, ethical, legal, security and social issues and responsibilities***.**

1. Identifies professional, ethical, legal, security, and social dimensions of a decision or action and its potential impacts on the individual, the company/organization, and the public.
2. Recognizes cost, schedule, and risk components in terms of ethical issues.
3. Recognizes and distinguishes between different or competing ethical perspectives.
4. Applies the standards of a professional code of ethics to determine an appropriate course of action.
5. Explains professional, ethical, and social considerations in a computing context.

F *An ability to communicate effectively*.

1. Applies standard rules of grammar, syntax and structure in written and oral work.
2. Demonstrates use of conventions particular to the discipline (e.g., organization, language choice, document type, source citation guidelines, and stylistic choices) in writing and presentations.
3. Demonstrates consideration of context, audience and purpose.
4. Correctly uses sources, examples, analogies, illustrations, and statistics to support claims.
5. Uses graphical materials (e.g., illustrations, tables, schematics, photos, etc.) to support and extend the verbal component of documents and presentations.
6. Uses delivery techniques such as posture, gesture, eye contact, enunciation, voice projection, vocal expressiveness to engage the audience during presentations.

G *An ability to analyze the local and global impact of computing on individuals, organizations, and society.*

1. Evaluates potential local and global impacts of computing technologies on individuals, organizations and society to make a choice, decision, or action.
2. Evaluates stakeholder needs and perspectives in local and global contexts prior to implementing computing solutions.
3. Analyzes local and global risks and uncertainties for individuals, organizations and society associated with implementing computing solutions in order to make a choice, decision, or action.
4. Considers the tradeoff between risk, uncertainty, and benefit.

H *A recognition of the need for, and an ability to engage in, lifelong learning*

1. Seeks and evaluates outside sources (possibly including personal experience).
2. Solves a problem using the specification of an unfamiliar software package, language or system.
3. Recognizes gaps in personal knowledge base and identifies what additional knowledge is needed, as well as methods for obtaining that information.
4. Analyzes personal biases and assumptions.
5. Makes references to previous learning and shows evidence of applying that knowledge and those skills to demonstrate comprehension and performance in novel situations.

2. Assessment Methodology

In order to assess student achievement of these outcomes, we employ a "direct" method in which we have student teams work together to address a real-world problem specifically designed to prompt for discussion related to various aspects of professional practice. In order to foster collaboration and discussion, we deliberately construct the problem to be open-ended, with no clear solution.

The problem was given as a course project in the spring, 2014 offering of CptS 402 ("Social and Professional Issues in Computer Science"), a required senior-level course in the BS. And B.A. in Computer Science degree programs. A copy of the project description given to students is provided in Appendix A. Working in teams of four to six, CptS 402 students had four weeks to complete the project by engaging in online "discussions of the scenario within the OSBLE[1] course management system, and ultimately submitting a policy statement (not assessed here).

The course instructor provided the CS Curriculum Committee (CSCC) with online transcripts of the discussions of all teams that participated in the assignment. The CSCC chair randomly selected the discussions of five teams for assessment. These transcripts, which are included in Appendix B, were made available to the other three members of the CSCC (Carl Hauser, Larry Holder, and Ananth Kalyanaraman) through an OSBLE course set up for ABET assessment activities.[2] Each committee member was tasked with independently assessing each of the transcripts with respect to the five "professional skills" outcomes presented above, and posting their ratings and justifications to an OSBLE "discussion assignment" specifically set up for this purpose.[3] For each outcome, committee members scored each discussion on a four-point scale with the following definitions: 1) Unsatisfactory, 2) Needs Improvement, 3) Capable, and 4) Exemplary.

In mid-May of 2014, committee members were given two weeks to perform their initial assessments and post their initial ratings and justifications to OSBLE. Once all initial

[1]OSBLE ("Online Studio-Based Learning Environment"; see https://osble.org) is a learning management environment being developed by Human-centered Environemnts for Learning and Programming (HELP) Lab, which is directed by the CSCC chair. A central studio-based learning activity supported by OSBLE is the critical review and discussion of problem solutions. Since 2012, an OSBLE course space has been the primary venue for CSCC discussions and assessment activities, which have taken place asynchronously. OSBLE course spaces has several features that make them well-suited for this purpose, including a shared filespace, activity feed, and the ability to create specialized "assignment" areas to support asynchronous review and discussion.

[2]Note that the transcripts included in Appendix B are annotated with committee members' comments, which provide further justification of their ratings.

[3]Note that the assignment was set up such that committee members could see other committee members' posts and discussion only after they had posted their initial ratings and justifications.

assessments were completed, the CSCC chair identified discrepancies in committee member ratings, and prompted committee members to further discuss areas of agreement and disagreement through a separate OSBLE "discussion assignment." That online discussion was closed in late June of 2014.

3. Results

Table I presents, on an outcome-by-outcome basis, the average ratings for each of the team discussions assessed. To provide further documentation on these ratings, Appendix C presents the committee members' discussions online discussions of their ratings and changes they made.[4]

Table I. Average assessment ratings for each of four randomly selected discussion teams by outcome (standard deviations are in parentheses)

	Outcome				
Team	D	E	F	G	H
1	2.3 (1.2)	2.8 (0.3)	2.7 (1.2)	2.3 (0.6)	1.7 (0.6)
2	3.7 (0.6)	3.0 (0.0)	3.3 (0.6)	2.2 (0.3)	2.8 (0.3)
3	2.8 (0.3)	2.7 (0.6)	2.5 (1.3)	2.3 (1.2)	2.2 (1.0)
4	2.7 (1.2)	2.2 (0.3)	2.7 (1.5)	2.5 (0.5)	1.7 (0.6)
5	3.0 (0.0)	4.0 (0.0)	4.0 (0.0)	3.7 (0.6)	3.7 (0.6)
Avg:	**2.9 (0.4)**	**2.9 (0.2)**	**3.2 (0.3)**	**2.7 (0.4)**	**2.4 (0.6)**

4. Discussion and Recommendations

The CptS Assessment Committee has established 3 (“Capable”) as the target rating for each outcome. Inspection of Table 1 suggests that this average rating met or exceeded the "Capable" target for only one of the five professional skills outcomes (F). With respect two outcomes, D and E, the target was nearly met (2.9); however, the average ratings of the other two outcomes, G and H fell well below the 3.0 target.

The flowchart in Figure 6 of the EECS Assessment Manual clearly describes our process for making recommendations based on the professional skills assessment results. Based on our 2013 assessment of professional skills discussions, outcomes E, G, and H were put on “watch.” Since Outcome E continues to remain near the "capable" threshold, we elect not to take any action with respect to this outcome, but will keep it on “watch” for the following year.

In contrast, Outcomes G and H, which were on put on “watch” last year, remained well below the "capable" threshold in the 2014 assessment. For this reason, upon further discussion, we recommend the following actions in order to address these continued deficiencies in professional skills:

- Consider adding a one or two-week unit to CptS/EE 302 in order to train students on how to analyze global impacts, identify areas of missing knowledge, and engage in self-directed research to address those areas of missing knowledge. If this suggestion is pursued, it will need to be done in close collaboration with the CptS/EE 302 instructor, who can assist in identifying a suitable curriculum for teaching these skills.

[4]Unfortunately, due to a technical problem with OSBLE, we lost committee members' original justifications of their ratings. Thus, Appendix C includes only the committee members' descriptions of how they changed their ratings after viewing the ratings of all committee members.

- Consider changing the assessment activity for Outcomes G and H from a group activity to an individual activity in which CptS/EE 302 students are prompted to write a report that requires them to demonstrate Outcomes G and H, and that is graded against these Outcomes by the instructor.
- Discuss the situation with the EE and CE Assessment Committee Chairs in order to see if their students are also demonstrating these deficiencies, and to seek advice on now to address them.

These actions will be added to the agenda for discussion at the 2014 faculty retreat in August.

Finally, Outcome D dipped slightly below the "capable" threshold in the 2014 assessment. While the CptS Assessment Committee does not find this to be overly concerning, we will put this outcome on “watch” for the following year, per the guidelines established in our assessment manual.

Appendix A:
CptS 402 Assignment Prompt

CptS 402—Social and Professional Issues in Computer Science Spring 2014

Team Project: Online Professional Skills Discussion and Policy Statement
Released: Tuesday, Mar. 25
Initial Posts Due: Thursday, April 3 at 11:59 p.m.
Response Posts Due: Thursday, April 10 at 11:59 p.m.
Policy Statement Thread Due: Thursday, April 17 at 11:59 p.m.
Final Policy Statement Due: Thursday, April 24 at 11:59 p.m.
Worth: 20% of your overall grade
Last modified: July 7, 2014

Overview

This team project is designed to assess your knowledge of, and ability to apply, ethics and professional skills. The overarching purpose is to determine how well the computer science degree program has taught you this knowledge and these skills. In addition to counting toward your CptS 402 grade, the CptS Curriculum Committee will assess a sample of the team discussions. When the CptS Curriculum Committee assesses these discussions, all names will be anonymized.

For this project, you have either self-selected a team of students, or you have been randomly assigned to a team. As part of this team, you will engage in an online discussion to capture your thoughts, perspectives, ideas, and revisions as you consider a computing scenario. Through this online discussion, you will engage in a collaborative exchange and critique of each other's ideas and work. The goal is to challenge and support one another as a team, so that, as a team, you can (a) tap your collective resources and experiences, and (b) dig more deeply into the issue(s) raised by the computing scenario. In addition to engaging in an online discussion, your team will produce a policy statement that summarizes your proposed approach to the scenario.

Scenario

As discussed in class, several new technologies, including GPS tracking, surveillance cameras and automatic face recognition technology, make it increasingly easy to track the movements and whereabouts of people who are out in the world. Given these state-of-the-art of these technologies, suppose that your team is considering the possibility of launching a new Internet start-up company to develop "webcam history" technologies.[5] Using the latest and greatest facial recognition technology, your company proposes to continuously process the images of surveillance cameras. Based on this processing, your technology would make at least two new features possible:

(a) You can present visual timelines that provide a historical trace of the camera images (and locations) of a given person.

[5]This scenario was inspired by a description offered by Georgetown University law professor Jeffrey Rosen on a broadcast of "The Diane Rehm Show." See http://thedianerehmshow.org/shows/2011-11-02/constitution-today-fourth-amendment/transcript, and refer to timestamp 11:30:52.

(b) You can support historical and spatial searches for specific people and places, e.g., "Where was John Doe at 5 p.m. on March 15, 2008?," or "Who was at the Washington Monument at 6:33 p.m. on January 3, 2010?"

Note that some surveillance cameras are operated by public agencies, and are presently available online. Others are operated by public agencies, but used only by law enforcement. Still others are operated by private agencies. In order to gain access to those cameras that are not presently available online, your company would need to develop contracts with these agencies.

Possible users of your technology are both (a) individuals, who could access your technologies through a public website you develop, or (b) government agencies, for-profit businesses, and non-profit businesses, which could directly or indirectly (by licensing your technologies) use your technologies.

As a team, your task is to think about, discuss, and converge on the specific kinds of technologies you should and should not support, the people and places that should and should not be included in your searchable database, and the users who should and should not have access to your technologies. To that end, you will need to design and clearly articulate your company's ethical and social responsibilities policies, which will be ultimately codified in your "policy statement."

Guidance on Ethical and Social Responsibilities Policies

Your company will be required to provide detailed information to its constituents on the ethical and social responsibilities policies that you will follow. You are expected to do substantial research and conduct discussions before designing these policies for your site. Your policies must be based on, but not limited to, the ethical principles, Code of Ethics, facts, data, laws, and frameworks discussed in the course. You are required to cite all external sources of information, both in your discussion and in your final policy statement. Examples of policies to consider include, but are not limited to:

<u>Users' Personal Information</u>

1. In addition to the Webcam History records, what personal information is collected from the user and why?
2. Do you have opt-in or opt-out option policies? If so, for what information?
3. How secure should your database be? Why?
4. How and what information is made available to law enforcement (government) agencies without a court order?
5. How and what information is used for user profiling?
6. What information is shared with (or sold to) third-party vendors?

<u>Access to your technology</u>

1. How transparent/easy to see/understand are your policies to your users?
2. Is any Webcam History information exempted from being collected, disseminated, or sold? Why?
3. Do you buy/sell Webcam History data? If so, for what purpose?
4. Is your technology available in multiple countries? What are the implications?

Project Timeline

You will have **four weeks** to complete the online discussion and produce a policy statement with regard to this scenario. To foster the refinement and maturation of ideas, ensure that you actively participate, and adhere to the deadlines described below. It is important to make your initial posts (and subsequent responses) in a timely manner. Your initial post, which you will compose independently, is due by **11:59 p.m. on Thursday, April 3.** You are expected to make multiple posts during each stage of this on-going discussion. The timeline below suggests how to pace your discussion. This is just a suggestion. Feel free to pace the discussion as you see fit, but note that your grade will be partly based on how well you adhere to these deadlines.

- *By Thursday, April 3 at 11:59 p.m.: Make Initial Posts.* All participants post initial responses that address the scenario prompt and take into consideration the issues raised in the "Guidance on Ethical and Social Responsibilities Policies" section above. These initial posts must be a minimum of **500 words**. Note that you are expected to write these posts *independently*, without consulting your other team members. You will not be able to see others' posts until you make your initial posts. These posts are intended to provide the starting point for your team's deliberations.
- *By Thursday, April 10 at 11:59 p.m.: Complete Response Posts*. Team members respond by tying together information and perspectives on important points and possible approaches. To that end, the team creates new discussion threads to address each the following (each discussion thread should be clearly labeled):
    - *Professional, ethical, legal, and social issues and responsibilities*. In this thread, engage in a discussion to identify professional, ethical, legal, and social dimensions of each proposed decision or policy. **The ethical frameworks and Code of Ethics discussed in the class must be enlisted to provide a rationale for and/or against each proposed decision or policy**. In cases where competing ethical perspectives or Code clauses are in conflict, the team should attempt to resolve the conflict by prioritizing competing perspectives/clauses and/or using its best judgment.
    - *Local and global impacts on individuals, organizations, and society*. In this thread, engage in a discussion that explicitly considers the local and global impacts of each proposed decision or action on key stakeholders, including individuals, organizations, and society. In addition, assess the certainty with which you can determine the impacts of each proposed decision or action.
    - *Further knowledge and research needed*. In this thread, engage in a discussion that identifies additional knowledge (facts, laws, statistics, etc.) that you need to know in order to make the best possible decisions or choose the best possible policies. Fill in the gaps you identify by performing research to seek and evaluate outside sources, making sure to cite each source. In cases where you choose not to perform additional research, identify appropriate methods you would use to obtain the information.
    - *Biases and assumptions*. In this thread, engage in a discussion to identify and analyze your personal biases and assumptions about the scenario. These biases and assumptions will be important to make explicit as you move toward identifying viable approaches and courses of action.

- *By Thursday, April 17 at 11:59 p.m. Complete Policy Statement thread*. Start a new thread entitled "Policy Statement," and use the thread to converge as a team upon a set of decisions and policies to address the scenario.

- *By Thursday, April 24 at 11*:59 p.m. *Submit Final Policy Statement Document*. Create a PDF document that brings together and synthesizes your team's final position. This statement should be at least 1,000 words, and be written as a polished essay in clear English. At a minimum, the statement should enumerate the set of policies and decisions your group would adopt, and clearly articulate your rationale for each one. Submit the PDF document through the "Team Policy Statement" assignment in OSBLE.

Assessing team members' contributions

You are required to submit a team member evaluation of the contribution of each member of the team towards the final policy statement. (We will evaluate each team member's individual contributions in the online discussions separately, so please consider only each member's contribution to the final policy statement.) These evaluations will be used to weight each team member's policy statement grades based on his or her relative contribution. All team members are expected to contribute equally.

Grading

You will receive both an individual grade for your contribution to the online discussions (weighted 70%), and a team grade for your policy statement (weighted 30%). The multiplier that results from the team member evaluations will be applied to your policy statement grade. Both the online discussion contributions and the policy statement will be scored using detailed evaluation rubrics available on OSBLE.

Appendix B:

Transcripts of the Sample of Online Discussions Assessed

Team Project Discussion - Team 07

Toggle Anonymity

Select Discussion: Team 07

Please see attached prompt and rubric.

Enter new discussion post here...

Post

Anonymous 2725
04/03/2014 05:46 PM

In addition to the Webcam history records, personal information like where the person goes,his daily routine, what he likes or dislikes and who the person he i dating with and in which bank he is an account holder can be figured out using the Webcam history, and pretty much everywhere he goes and what he does c be can be collected.All the above can be considered as personal information.

Our company would definitely have an opt-in and opt-out policies which allows their customers to choose between right to privacy or users explicitly give the permission to share their webcam history records and personal information with others which will be very useful when someone is murdered ,or kidnapped et and help to reduce crime. This information used by advertising agencies through common search or the through commonly visited in things on the internet.

The database should be very secure because our company will hold a responsibility to keep the information stored in the database securely because there a lot of hackers out there who have lot of experience hacking different servers to access the data stored in the servers and also there are people out there who have chosen opt out policy because they want to keep their information private.

The government agencies or law enforcement can contact our company to access information of the people to solve cases or can be the evidence for some case. The government agencies cannot just ask for a person's information or routine work recorded in the surveillance camera just because they have power they can get information only regarding an investigation. A users routine schedule or the activities he would perform in regular basis and thing that the person interested in. Our company will be willing to share or sell information of users who have opted in only with the third party were only government agencies is considered as third party.

Our summarized version of the policies will be written in just few bullet points. For anyone who wants to know more information regarding on particular policy i specific, can go and read the detailed description as stated in the policy. This is done so that it is easy for the users to understand the main things without having to read the complicated document.
Some webcam history information like what happened inside a person's house or a bedroom should obviously be exempted from collection such kind of data or even selling this kind of data. There should be some level of privacy.

We would probably not want to buy webcam history. But may be sell the information to government agencies as this would mostly help them solving cases and is not a good idea to sell the webcam history to anyone else as it could be easily misused. Yes this kind of technology is used in multiple countries for maintaining safety in crowded public areas. This is also used in many countries that have very bad weather conditions. This kind of technology has its own pro and cons and how people use it.

Anonymous 2731
04/03/2014 06:09 PM

As a start up company interested in developing a "webcam history" software solution, there are many important things to consider in order to make this softwa ethically acceptable. Within the history records, personal information would be collected about users such as name, image, and location history for the application to function. However in my opinion, in order for this to be ethical, it would need to be opt-in for these specific users in order to treat them as rationa beings. If this were to work, if users did not opt in it would still record their image, but the system would not be able to identify them based on name; the systen would probably save the image and history under a codename. I believe that the database should be secure to prevent people from getting or changing information, but it should not be the primary focus, as the information would be publicly accessible in some situations. Information to law enforcement without a court order would be only the same information that the normal users would be able to get, or history of images of people, but with codenames. User profiling would consist of a high quality image, Name, and collection of history. In my opinion, the best way to deal with third-party vendors would be similar to facebool where we would provide the information on users, but not give them any information that identifies users unless the users agreed to it as well.

As far as access to our technology goes, I would like the policies our company has to be easy to see and understand to the user, perhaps have 2 versions of EULA, one that contains the full legal text, and one that is a summarized version for users to better understand it. Users that wish to know everything they agre to could read the full EULA, while those who would like to skim it but still know what they are agreeing to could read the shortened version. I would say there a certain webcam history information that should be exempt for being collected, disseminated, or sold. Personally, my stipulations on this matter are that history that occurs out in the public can be collected, disseminated, or sold; history that occurs in semi private areas (in houses/etc) can be collected but not sold, an finally history in private areas (such as bathrooms) cannot have any of those actions done. I believe that buying/selling webcam history data could be beneficia to multiple parties, but it would highly depend on the company we would be doing business with and if the users knew about it. For instance, selling user

1. Writing not great -- ok for blog post. Hits the high points. No indication yet of what's not known. *[hauser]*

2. **(image annotation)**
- no sense of discussion in general (mostly operating as individuals than a team)
- quality of English: colloquial in most places
- no evidence of arriving at conclusions/consensus
[ananth]

information to an dating websites would be violating user privacy, but selling user information to advertising companies could help the company tailor advertisements to better suit the user, assuming the user was ok with this. I would say that the technology being available in multiple counties would make it more usable for a higher number of users, but that also brings up questions about who can access data with regards to location.

Anonymous 2707
04/03/2014 10:07 PM

People take webcam privacy very seriously. If I were part of a start up I would have to ensure that my company followed several ethical frameworks to not impede on people's privacy. Since my company would want to work with webcam history we would have to take extra measures to ensure that the privacy is kept. My company would need to track location to have accurate webcam history for a given user. We would also need some form of identification like a uniqu username and/or identification number. If we wanted to take it a step further we could include first name, last name, phone number, and email. The user shoul have the choice to opt in on what is displayed and stored by the company. For example a user that wants to use this service would have to opt in to location a have the choices to opt in to display username, first name, last name, phone number and/or email. This way the user has the choices necessary to cover priva issues that might occur with their personal information being gathered. If the company went with an opt in method, any information gathered would be ethical b Social Contract Theory since they would have to agree to the contract to use the service. I personally think the database needs to be very secure, especially if we are taking the opt in method. We ensure through a contract that only that information the user wants to be gather and/or available to be access by other people, especially people outside the company. I personally think that a court order should be required for the information to be access outside the company I if there was a certain law that requires differently for higher up government agencies to access the information. My reasoning for this is the user would have signed a Terms of Use contract and we as the company need to uphold that contract or we will violate the Social Contract Theory. User profiling would require username, email and password. Additionally information such as first name, last name, and phone number could be stored for the profile. We can also include profile picture to give the user a little customization for their profile. We will give the user the option to decide what information will be shared with third parties Generic information such as user concentration can be shared as long as no personal information is given away without user consent. I think that we need to make our policies extremely clear so that the users completely understand what they are agreeing to. If there is any information the user doesn't want to be saved there should be a "private" mode. Many people have times where they don't want anything tracked and we as a company should give them the option t temporarily disable the tracking software at any time. To get an idea of what we would need buying webcam data for research purposes should be fine but selling data other than statistics would be unacceptable. I think this technology should be available in multiple countries. The only issue with this is keeping the privacy laws from different countries from being violated.

Anonymous 2707
04/10/2014 04:10 PM

Professional, ethical, legal, and social issues and responsibilities

Anonymous 2707
04/10/2014 04:16 PM

From a Kantianism standpoint I think this is unethical. Not everyone is agreeing to the facial recognition and therefore not being treated as rational beings. From a Social Contract standpoint this can be ethical since users can agree to be included in the software, if the company goes with an opt-in situation.

Anonymous 2731
04/10/2014 04:23 PM

I believe that ethically we should have it setup that people can't obtain the user information unless the user has specifically approved to have their information be public. In this way we wouldn't be treating our users as a means to an end, and would be ethically sound under kantianism. Of course, we would need to allow government and law enforcement to use our services, as we obliged to due to social contract theory. For the good of the public, having a history of locations would be sound under act utilitarianism as it would help law enforcement and therefore help catch criminals. In order to keep users happy, we could also only allow law enforcement to see history of people or locations, and publicly we would not display this information.

Anonymous 2707
04/10/2014 04:48 PM

At the very least public and government locations would be fine in my eyes. They run these locations and by at least ethical egoism are free to record what they want there.

Anonymous 2725
04/10/2014 07:21 PM

As our company is going to have an opt in and an opt out policies for the users to choose between the two. Users, who choose opt-out policy will have a right to privacy of their information and will not be disclosed until some sort of court warrant is issued. So our organization is not treating the users as means to an end rather users are treated as rational beings(ends in themselves) . Hence it is ethical according to Kantianism ethical framework .

Anonymous 2731
04/10/2014 08:53 PM

1
I agree that public and government locations would be the best places to have the system running, especially if we were to notify people somehow (through signs or a notice) that they were being recorded. I definitely agree with the opt-out policy Shwetha brought up too, it seems that it would be fair to the users, and not treating them as a means to an end.

1. **agree**
Up until now there was not really a follow up in the discussion. Individuals seem to be making their own statements without feedbacks. (outcome D3) *[ananth]*

Anonymous 2707
04/10/2014 04:11 PM

Local and global impacts on individuals, organizations, and society

Anonymous 2707
04/10/2014 04:35 PM

Some people might be wary of cameras recognizing faces initially. The government would love this for tracking people of interest but they can encounter backlash for creating a Big Brother type scenario. The companies that would have to be contracted for their cameras could encounter backlash for allowing this system through. Foreign citizens might be confused by this if not implemented in their countries and would cause issues in the program with error flags. Foreign governments might be afraid of what else is being recorded by this software.

Anonymous 2731
04/10/2014 04:51 PM

Local impacts: individuals- Could use the software and feel it is useful and worth the drawbacks, for example to find out how crowded it is historically at certain places. Also could feel like their privacy is being invaded. Fairly confident about how this would effect the users.
Our Company-Make money and help out the government while providing a useful service. Could also hurt the company by releasing this product if done poorly, due to user outrage. I'm pretty certain that this would be how it would happen.
Government- Would help find criminals and could decrease the amount of crime. Certain about the finding criminals, not sure about decreasing crime, it hasn't historically done much.
Society-Could change crime rates, and make people much nicer in public. But it could also make crime move to private settings instead, where they can't be monitored. Pretty certain, initially it could help but crime would likely find a way to happen.

Global Impacts: individuals- Individuals at home would not feel happy being able to be monitored by others, feel privacy is breached unless a contract was signed with permission. Pretty certain on this.
Terrorist organizations- Could provide them with information on when and where to hit. My certainty on this is a bit unsure, but it is definitely an option, terrorist organizations like to attack at public places, and giving information on how populated places are at certain times/days would not be helpful towards preventing attacks.
Society-Could face boycotts on software from other countries, especially if their laws and policies on privacy and data collection did not agree with ours. This I am pretty sure could happen, some companies face this today even, so our software could illegal in certain countries.

Anonymous 2725
04/10/2014 08:42 PM

The global impact on having surveillance cameras recognizing faces has its own advantages for solving crimes, court cases, helps in tracking criminals, providing safety for people with political power like politicians visiting different countries and to catch criminals hiding in any corner of the world. Big organizations and companies also use surveillance cameras in banks and big companies for the safety of their employers and customers as well from robbery, any criminal activity and terrorist. Society also need this to protect women from may be sexual abuse and protect from criminals.Local impacts- Surveillance camera in grocery store or electronic goods store monitor the employees as well as their customers in case someone tries to steal something. Big public places like campus, malls etc for public safety.

Anonymous 2725
04/10/2014 09:52 PM

For more on the local impacts the organizations have a way to make some money and provide service the government is a goop point out by Derrick.

Anonymous 2707
04/10/2014 04:11 PM

Further knowledge and research needed

Anonymous 2731
04/10/2014 04:34 PM

In developing a privacy policy, knowledge of how privacy concerns are handled in current applications would be a huge help. For example, Google Maps is a similar service in that it displays images of pretty much the whole world. The way they are able to get around keeping these images is they use only images of public roads or areas for street view, it is not a live feed, and images of people and license plates are blurred. In addition, users can report concerns and ask for additional image blurring. Our system could apply similar stances such as only public areas and if not people must be informed there are cameras, blurred images (with saved real images for police), and additions for users to request more blurring on images. Of course we would have to come up with how long we would keep searchable data for the public out, and how long we can legally keep data on our servers, so more research on laws/current stances of similar products would be useful.

Google maps privacy policy: http://www.google.com/maps/about/behind-the-scenes/streetview/privacy/

Anonymous 2707
04/10/2014 04:42 PM

If we can find anything about it I think looking into what the government can access from a companies data is something to consider.

1. **monitored. Pretty certain,...**
2731 is very sure of his/her opinions and tends to treat them as facts rather than something to be questioned. *[hauser]*

2. **For**
no attempt on arriving at a consensus or closure for the arguments made. Team operating like a bunch of individuals. *[ananth]*

Anonymous 2707
04/10/2014 04:53 PM

Sunsetting the data I think is a really good policy. We can also include a "remove me" option or something similar to give the user the option to either blur their face or just remove the entry from the publicly available image.

Anonymous 2731
04/10/2014 08:55 PM

Definitely looking into what access government has on similar products would be a good idea. Sunsetting the data, at least for the general public to view would make sense.

Anonymous 2725
04/10/2014 11:00 PM

"Remove me" kind of option as Kyle said is good option to have.

Anonymous 2725
04/10/2014 11:24 PM

As we are taking about face recognition software processing images in surveillance camera, it is important to consider that people act differently when they know that they are watched especially the criminals would probably know how to avoid surveillance camera or cover their faces completely. So according to American Civil liberties who are still trying to figure out if this can actually increase safety and security. As the current facial reorganization software is not completely reliable it would possibly pose a treat to innocent people. Hence it is definitely things to consider.

Source : Face Recognition -https://www.aclu.org/technology-and-liberty/qa-face-recognition

1. **As we are taking about...**
Sloppy to the point of incomprehensibility. *[hauser]*

Anonymous 2707
04/10/2014 04:11 PM

Biases and assumptions 2

2. **Biases and assumptions**
Almost completely NOT about biases and assumptions (of which there are many expressed above but not recognized as such). Rather, more technical discussion. *[hauser]*

Anonymous 2707
04/10/2014 04:21 PM

Assuming that the security cameras have a high enough quality to get a readable face for the software. I also think that this could be incredibly effective in catching criminals but that requires a database of criminals to check against. For the average user I don't think this is needed.

Anonymous 2731
04/10/2014 04:27 PM

One way to get around the image quality is to have users opt in, which we could assume that when the government takes your fingerprints they take a high quality image for the system to check against. I feel personally biased in that the cameras would be a good idea if implemented properly but am skeptical as to the impact they could have without the data to support the background checks. Perhaps blurring faces on images that are displayed would be helpful, while keeping the non blurred copies saved in a secure database.

Anonymous 2707
04/10/2014 04:28 PM

I also am worried about false identification due to experience with other facial recognition software misidentifying accounts.

Anonymous 2731
04/10/2014 08:59 PM

False identification could be an issue, but with an opt in strategy we could get around that with higher quality photos to base the identification on. Also, it's pretty common with facial recognition to give a %certainty, so even if we had a match they wouldn't be able to be 100% sure it's them in most cases.

Anonymous 2725
04/10/2014 09:41 PM

Also the other thing to be worried about is how well does facial recognition software differentiate twins or some people who have very similar facial features. Innocent people can be greatly affected if they were to be mistaken with a criminal.

Anonymous 2725
04/10/2014 09:58 PM

Oh I did not see that Derrick had already mentioned about false recognition.So I want to add one more thing that is is what if people have got some facial surgery or if they have completely changed the way they look. How well is this software reliable...

Anonymous 2725
04/15/2014 10:55 PM

Policy Statement

Anonymous 2725
04/15/2014 11:12 PM

Users have an option to choose between opt-in and opt-out policy.[1] On choosing opt-out policy, the user's will have a right to keep their information confidential and their information/surveillance recording will be disclosed only on a court warrant. For user's that that choose opt in policy, their information would be shared to advertisement agencies and legitimate agencies(grocery stores,etc) for a useful purpose.

Anonymous 2731
04/17/2014 02:06 PM

I definitely agree with the opt-in/opt-out policy. I believe this is the best way to handle the privacy issues. During the opt-in portion, we could take a high quality image which would greatly reduce the false positives. With the opt-out policy, we could remove the ability to search for that person specifically for the public, but like Shwetha said, allow legitimate agencies use the data if needed.

I also think we should implement blurring of faces for the public to see unless the user has opted in. We should decide on a timeline to keep the history up for the public to view, I believe that 1-3 months would be a reasonable time frame to keep the data up for the public. We could then sunset the data for the public, but keep data on our servers if the government/police needed the data, as well as make the data non-blurred images on the backup.

Anonymous 2707
04/17/2014 03:00 PM

I think the wording for the opt-in policy is a little off. I think it should be more like "Users have the option to opt-in to this software. Until they opt-in the software blurs them out." We do need to keep all the data no matter how old since the government could use our data for criminal cases. Sunsetting the public data is an amazing idea and I think 1 month should be plenty. I'm fine with the ad sharing but we could offer an option to disable that for users. The hi-res photos is a great idea to counteract false recognition.

Anonymous 2731
04/17/2014 03:35 PM

Yeah, the opt-in policy should be reworded in that way. So in general it seems that we have agreed on "Users have the option to opt-in to this software. Until they opt-in the software blurs them out.". Also, the data that public can view is from the current date up to one month before, anything after a month prior would be invisible to the public but stored for government to use legally. Opting out would include the ability for the public to search for that person and also would disable ad sharing. Finally, opting in would allow hi-res photos to be taken to allow for reduced false positives.

Anonymous 2725
04/17/2014 06:31 PM

High resolution photographs is a good way to go about reducing false positives for opt in users as Derrick mentioned, But just to make it clear, the surveillance recording would have high resolution recording without blurring the images on court order because they need to see all the people no matter whether they have chosen either opt in or opt out policy correct?

Anonymous 2725
04/17/2014 06:39 PM

Sunsetting the public data for one month is a good amount of time that Kyle mentioned above. And definitely it should be a part of the policy statement as the public accessing the data should be aware of how long they will have the access to the data.

Derrick yes, I like your rewording. I think we can have that along with some additions or modifications I guess.

Anonymous 2731
04/17/2014 08:04 PM

Correct, my idea on the high resolution images is that they would be saved would be nonblurred on court order, since if it was a legitimate government concern it would not matter if they opted in or out.

As far as the one month sun setting, we should definitely make that clear in the user agreement, in addition to the other polices we have agreed on. I'm open to other suggestions too though, I'm sure there are other portions of the policy that could be added to or worked on.

Anonymous 2725
04/17/2014 11:10 PM

1. **Users have an option to...**
Does this make sense?
[hauser]

2. **We do need to keep all...**
Contradictory! - but refined later.so as not to be.
[hauser]

3. **High resolution photographs...**
I am kind of amazed that they accept that government has a right/need to these data w/o question as long as access is governed by court order.
[hauser]

Ya we can work on coming up with other portions too.

1. Teamwork: the students interacted with one anothers' comments and seem to be on track to produce the required product. *[hauser]*

Team Project Discussion - Team 01

Toggle Anonymity

Select Discussion: Team 01

Please see attached prompt and rubric.

Enter new discussion post here...

Post

Anonymous 2733
04/03/2014 04:36 PM

I think that the technology our company is developing would be pretty awesome. However there are several issues that could arise. First off like we discussed class on Tuesday, false matches. The technology used to identify an individual would have to be some sort of next generation extremely accurate facial recognition technology.

Usually in order to make a confident facial match you have to have a high resolution straight on picture of the individual looking into the camera. A vast majorit of the people in the United States already fall into this category because of driver's licenses. However DMV records aren't public so would our company have make a deal with the government? If we did manage to get a contract with the government would there then be an opt out form that people could file that would prevent us from matching them?

Next, what about people that do not want to be found, for example people in the witness protection program. Would we allow the government to remove those people from our system? Would be the general population be able to use our system, ie a website we develop?

As for places that we would not allow our technology to work, probably the main concern would be private property. However if a camera is on public property and can see into your private property is there a potential conflict? "Surveillance" now does things like that, sitting on a street in front of a house and observing people in their homes or on their own property. However the "respect the rights of others" section of the code of ethics would be a factor in this. In residential areas I think that it would be best to not monitor people because they should have a right to privacy when they are not in public anymore.

I think our policy statement would have to be extremely transparent and as easy to read as is humanly possible. Kind of like how paypal does their policy and gives the highlights as bullet points every time they update a section.

Pertaining to how we will get access to the webcam data, obviously the public ones are easy. As for the law enforcement cameras, our aforementioned contra with the government would handle those. I think we would have to make contracts with a lot of private companies to expand our coverage. Maybe in our contra the private company would have to disclose somehow to the people that they would be monitored while on their property or under certain circumstances. The code of ethics would certainly back up the informing of others under the "Disclose information that others out to know" section. In order to fund the cameras fr the private companies I would think that we would have a website available to the public and maybe sell webcam histories on a per search basis?

I know a lot of my post is questions but I think that is because these are a lot of the things that we need to figure out over the course of this assignment before make our policy statement.

Anonymous 2715
04/08/2014 04:26 PM

I agree that it is a concern in places of private property. However, there are some public places that cameras should not be installed. For instance, a bathroom in the recreational center should not have a camera installed even though it may be a potential place where illegal activities may happen. I agree to your code of ethics that we should "respect the rights of others" and this have to be applied to my statement as well. In general, there are public places that should also not be allowed for camera to be installed as it is not ethically right to do so.

Anonymous 2718
04/09/2014 09:06 PM

I agree with Micheal that there are certain public places that should not have cameras. As I mentioned in my initial post, I think schools should be exempt because it is a role in society to protect children. I agree that our policy statement should have bullet-ed statements that make it easier for the public to read, however we may need more wordy sections of the policy to protect us legally. I also agree that our service should be something that people pay for, seeing as that will best fund an increasing system of webcams and allow us to use the most up-to-date technology.

Anonymous 2718
04/03/2014 08:48 PM

In addition to webcam records our company would also collect names, photos, and hometowns from users. We would use these photos to improve the

[no notes on this page]

database that facial searches would run through. We would use the names so that we could reduce the risk of a person being wrongly identified by the softwa The use of hometowns could be used to reduce the number of people to be searched when a location is not a tourist destination. We could also use the hometown data to allow users to only let people in their hometowns search for them on the database.

In our company's policy we would let users opt-in to our services. To do otherwise would be a violation of the public's privacy. Making our services opt-in woul also be following the code of ethics by respecting the rights of others. An opt-in policy would also protect people who may not want to be searched; victims of stalking or high-profile people such as celebrities and politicians may not want the public to have access to a system which will give tell them places where the like to go frequently.

As a part of the opt-in policy, we would ask users to grant us permission to put them into our searchable database. We would also ask for the user to provide quality picture that can be linked to their name to reduce the risk of them being misidentified.

It is the responsibility of our company to protect high risk targets and we may want to choose an option for such people to keep them from being put into our system without consent. If a person can provide a valid reason why they should not be in our system, such as a person in the witness protection program, we could take a reference picture from them and any time another user wished to put a picture that matches the face of the provided one we ensure that the pictu will not be admitted.

To protect the privacy of all of our users it is our duty to ensure them that our database has top notch security. Many people are concerned with their privacy a would feel uncomfortable participating in a system that was not secure.

Without a court order our company should allow law enforcement officials access only to camera feeds that are public or feeds that we have received from the By allowing law enforcement access to our cameras which were provided by them or public, we may be able to work better with them and convince them to gi us access to more security camera feeds such as the CCTV cameras installed in New York City as a part of their "Domain Awareness System"[1]. Additional by granting law enforcement use of our software in the case of cameras that are provided by them or public access we are still respecting the rights of our use because law enforcement could access those feeds on their own without a warrant.

As far as third party vendors are concerned, users may be uncomfortable knowing that we sell their information. However, in order to make deals with some companies to gain access to their cameras we may have to provide them with information. In that case I propose that we could provide information to businesses about the customers that shop there and how often they visit the business. This policy may be acceptable to our customers because if they freque a business, the vendor could use loyalty card and credit card records to determine if they've been to that location.

In order for our policies to be fully complete and protect us in a court of law, they will likely have to be like most other policy statements and difficult to understa by users. However, in order to follow the code of ethics and fully disclose information that others ought to know a simplified policy statement should be made available. Using Kantianism as a defense for this, to do otherwise would be treating our users as if they are not rational beings. To respect the rights of our users and treat them as they ought to be treated, we must provide our users with a policy statement that they can understand. In this statement we need to ma it clear, what their information can be used for, what information they will have access to, and what protections we offer them.

Anonymous 2718
04/03/2014 08:48 PM

Webcam history pertaining to high risk targets, who can provide a solid reason as to why they should be exempt, should not be collected. This policy should be put in place to protect the identity and habits of people who need protection. Such people should include but not be limited to witnesses under federal protection, celebrities, international dignitaries/diplomats, and stalking victims. Additionally as it is our societal duty to protect children, we should not collect or store any information on minors.

To make our network as vast as possible, we should be open to purchasing webcam data. This will allow us to cover a wider area; however, we should consider the possibility of locations that we would not collect data from such as schools and playgrounds. Additionally, we should consider being willing to sell back our data to businesses in exchange to access to their webcams as another way to expand our coverage area

To begin with our services should not be available in different countries. It will be easier to set up a network in the United States first, and then look into expanding globally. Additionally if we do choose to offer our services in a foreign country, we would need to look at U.S. foreign policy with those countries. Additionally we may want to limit the locations a user can access to their own country.

[1] http://www.theverge.com/2014/1/25/5344380/new-york-city-police-install-200-security-cameras-to-guard-against-super-bowl-terrorism

Anonymous 2733
04/08/2014 04:23 PM

I certainly agree that opt-in would be the best option for keeping to the code of ethics. Your analysis maintains more strictly us staying as our own private company where mine kind of integrates us with the government. We will certainly need to decided on which path we would rather take.

As for each individual submitting a high quality picture of themselves there are maybe a couple issues. How can we be certain that the picture is in fact of themselves, and two would we have to make a system that rejects low resolution photos or maybe photos that aren't lit well enough? My idea of using the DMV to supply our pictures would solve both of those problems because the DMV takes high resolution, straight on, lit photos with a solid color background.

My list of people that should be protected was more restricted to only WitPro but I like all your ideas for people that should be exempt. However your opt-in idea seems like it would already protect these people by default.

I agree with your limitation of the program to United States only and that only people in the US can use our program. I think for this assignment we should stay limited to the United States only. However if we have an online interface that tries to restrict its users to the United States only, people could get around it in multiple ways and is really only an inconvenience. We should probably just ignore that part and let anyone use the website.

It would seem that we agree on our policy statement having to be pretty readable. Even with a simplified version of our policy statement that would

[no notes on this page]

cover all laws and liabilities, I doubt it would ever get read anyway. However I think it would still be our duty to supply as simple as one as possible.

I love your idea of only supplying the law enforcement with access to webcam history on cameras that are public or that we received from them. We would supply a service that they would be able to do themselves by brute force and save them a lot of time. With a court order we could expand our search to include the privately funded cameras.

Anonymous 2715
04/09/2014 07:37 PM

I agree that our software should have an opt-in policy for the users. This will enable our software to be better and protects the public's privacy as you mentioned in your post. I also agree that the law enforcement are allowed to camera feeds that are posted by users and require a warrant for accessing to our database for items that are collected privately by the software. However, a warrant is also needed to access to our live cameras. Since this software is capable of tracking people down by searching their name and or places at times, if we are able to create a contract with agencies who have surveillance camera set up and allowed us to access and store information from the camera, law enforcement will require a warrant issued to access directly from us. This is to ensure that the public's privacy and our agreement with the users are maintained. Using Kantianism, we will see that the company is using the user as a mean to one's end. Hence, a warrant will make the whole process ethical.

Anonymous 2718
04/09/2014 09:17 PM

Justin:

I like your idea of using DMV photos to ensure that people are who they are claiming to be. If we were to contract with the government we could work out some way that the opt-in policy is connected to their driver's license. I agree that preventing people from outside the U.S. from using our website would be fairly difficult, however if everyone was to opt-in using their driver's license before being allowed to access web cam data, I think that would help in restricting access.

Michael:
I agree that a Kantian analysis shows that a warrant should be required for access to our privately collected feeds.

Anonymous 2715
04/03/2014 09:54 PM

This technology can be used for many reasons that can be applied to. It is use in for surveillance camera, GPS tracking or even face recognition. Its main purpose is to be a platform where people can find webcam history of other. However there are other features implemented in this software as well. It is capab of integrating the software into VoIP software or smartphone camera or anything that has a camera and/or Internet in one device. Another feature is allowing user to find other people of their past location and visual timeline of camera images. It also has a search bar that allows user to find historical and spatial searches for a specific people and places. This versatility allows the program to attain a webcam history of a user or people easily. Other personal informatio that can be collected will be information from Facebook or any social media as this software allows a user to sign up by connecting their social media accour Hence, information such as name of person, date of birth, current and past location, and address, photos that are posted in their social media account, and phone number that they have input to create their account will automatically be added into the database. Under social contract theory, we will find that collectic of such information will be ethical as it is our company's right to attain these information when the software is being used.

This software allows user to sign up and use it through a website. Users are allowed to see other people's webcam history or being searched for their past location through the search bar. However, they will not be able to download the images or webcam history. To prevent downloading or saving using third party software, our company's software will have additional implementation that will black out the images or webcam history. For those who have signed up, they wi be given an option to be allowed their webcam history or images to be looked up by other users. People who have not signed up, are automatically opt-out. However, videos and images are still stored inside our database. Other information will be available to all, in other words, only videos and images would be hidden from other users if user choose to opt-out from being searched. The reason of user who are not signed up are opted-out because of Kantianism. If we create a universal rule that if a person does not know about this software, he or she shall not be able to be searched by the public which will be ethical.

Our policies regarding to our software will be transparent and as friendly as possible to the user who is going to use it. It will require all user to read the compa version of our policy which will provide all the main points from the main list of policies. This is to ensure that all the policy documentation of the product is give and shown to the user before they are able to use it.

All webcam history or images will be collected and stored in the database with an exception of government work or court order. Images or videos that are located in places such as bathrooms would automatically be hidden from public. Using Kantianism, we can create a universal rule that we should not allow inappropriate actions to be displayed in public. Images and videos will be hidden for those who opt-out from being shown. Our company will buy webcam hist from other companies whenever possible to create a more accurate location of a person and also to be the main platform that law enforcement would use to track down criminals. This software will be available in all countries. However, the system of tracking down users would be only installed in the United States.

In conclusion, this software will sensor all the inappropriate images or webcam histories. However, information are stored into the database for law-enforcem agency. Using act utilitarianism that this conduct will be ethical. It will be easy for law-enforcement to track down criminal and arrest the person which will crea our society to be safer than before. It also allows vendors to know what are the users or peoples' interest and allow them to modify their approach when they a planning to create or do something new. The down side would be that people will also feel unsafe at the same time as they can be watched for the doings online. However, there are more advantages than disadvantages which will allow this software to be ethical.

Anonymous 2733
04/08/2014 04:42 PM

It would seem that your requirement for the use of our product by law enforcement agencies is more strict than either mine or Alex's, are you saying that the only condition in which law enforcement can use our database is with a court order?

1. **This technology can be...**
Writing in this post does not match the quality of 2715's earlier post. ??? *[hauser]*

I hope there aren't many cameras watching us in the bathroom, although I have never really checked for them.

Also I'm a little confused as to your method of storing all the information. Are you saying that when we receive new information or pictures/video we should immediately sort through the data and identify every person that is identifiable and update their personal webcam history that is stored on our server? I was thinking that we could store the footage and then only parse through the data when we query a search for a specific person, so that we aren't making webcam histories on people that are not opted-in to our product.

Anonymous 2733
04/08/2014 04:47 PM

Although now that I think about it, maybe the updating of webcam histories, instead of storing tons of pictures and videos, would be way more efficient and much easier to sell on a website. Also we could start a persons webcam history based on when they opt-in to our product? However this would severely reduce the helpfulness to law enforcement agencies because unless that person was opted-in to our product there wouldn't be any webcam history on them, unless we stored all the footage on our server. Which brings us back around to my idea.

Anonymous 2715
04/09/2014 09:17 PM

Law enforcement only require a warrant when they want to access to the camera and see it live or access to information that the user have not put up since I believe that user's images and videos should be stored whether or not they have opted-in. Hence, by using Social Contract Theory, we can say that it is not invasion of privacy if people do not have the right to see unless is within the law that the data of a user has to be surrendered.

I believe that we should explicitly mention about putting cameras in public places. As you said, we do not want to have cameras in places like bathrooms even though it is public, it is not right to surveillance people then. Hence, I believe that people have the right to know that our software will filter out inappropriate images,

Anonymous 2718
04/09/2014 09:36 PM

I'm fairly certain it's against the law to have cameras in bathrooms/changing rooms. Often, if surveillance is needed, cameras are placed so that they can so who enters/exits but cannot see into the bathrooms themselves.

Are you saying that law enforcement should be required to provide a warrant even in situations where they've provided us the camera feeds? This would seem unnecessary since they could easily spend the time to comb through those feeds themselves.

I think in regards to storing webcam history, we shouldn't keep webcam data for people who haven't opted-in to our policy. I think doing so may cause the public to feel that we are not respecting their right to privacy. If law enforcement has a warrant to search for a certain person who hasn't opted-in to our policy we could obtain a photo from them and then use it to search. It would take more time, but be more respectful of privacy rights which will make the public happier.

Anonymous 2733
04/10/2014 04:51 PM

.:*Further knowledge and research needed*:.

Potential knowledge needed for our companies endeavors in the future could be assessing the interest of private companies to see if they would be willing to sell their camera feeds to us. Also the interest of the U.S. government in creating a partnership. There is no way to research if these things would be possible because we aren't really the owners of a company, however I feel like the U.S. government would be all over spying on people.

Research that might need to be done is how accurate we could get our technology. Maybe setting standards for our face match technology to prevent false positives and what percentage of false positives is deemed acceptable?

Anonymous 2718
04/10/2014 05:22 PM

I agree that we would need to research how willing other parties are to work with us. If others don't want to provide us with camera feeds then it will be fairly difficult to create a large database. I think if we were willing to market this to other companies as a way to collect market research, such as what stores a person visits, do they visit competing stores and whatnot they would be much more willing to work with us. Also if we can ensure them that we are not infringing on the rights of their customers we will have a much more convincing argument.

Would we include the percentage of false positives in our privacy policy? This would follow the code of ethics, disclosing information that others ought to know.

Anonymous 2715
04/10/2014 10:02 PM

I agree with your statement that we will not be able to research this extensively due to the fact that we are not a company and unable to do the calling and asking if a company who collects data will be willing to share or sell them to us. However, I believe that we can do our best in researching the statistic of company who are selling data through Google. Also I think we could research upon other companies who are doing face recognition program and see what are the accuracy of recognizing a person through just a few pictures.

[no notes on this page]

I personally believe another factor that we can research upon will be polling from people if such a technology will be ethical and asked their opinion on how to make it ethical if they think it is not ethical. This way, by Kantianism, we are creating a universal rule that with people's opinion we can make this software ethical by their suggestion.

Anonymous 2733
04/10/2014 05:16 PM

.:*Biases and Assumptions*:.

After re-reading my initial post I seem to be biased towards involving the government with our company in order to further advance both our access to a documented list of our targeted group of users and cameras to employ our product with.

Some assumptions that I've made include that the U.S. government would in fact be on board with contracting us, and that private entities would be willing to s their webcam feeds. If neither of these things were true then all we would have is a product that could be run on public cameras only and would probably have huge gaps in time between documented sightings.

Anonymous 2718
04/10/2014 05:33 PM

We do seem to lean towards a relationship with the government, however I feel that it's a necessary angle. In order to improve our product we need access to cameras set up and run by the government. We can also use this as way to help law enforcement agencies track down suspects, protecting the people in a community.

I think we have to run with the assumption that the government and other companies are willing to work with us. If not, then our product is seemingly useless. If no-one was willing to work with us would we have to simply charge a higher fee in order to set up cameras of our own?

Anonymous 2715
04/10/2014 10:10 PM

I agree that we are leaning towards law enforcement as an argument to make this software ethical. This software do not make much sense if it is applied for individuals finding each other as we have social media such as Facebook or even Googling their name, will show up as a result. Even though companies may benefit from the data that we have collected, I think that this software is most beneficial in tracking down criminals which is what law enforcement agencies do.

We do make an assumption that other agencies including law enforcement and private agency are willing to sell their data and continue using their camera for our data collection. If this software is going to be the main platform for law enforcement, we have to get all or at least 99% of private agency to work with us. Also another assumption that public agency cameras are automatically allowed to be used in our data collection.

Anonymous 2715
04/10/2014 05:33 PM

<-- Local and global impacts on individuals, organizations, and society. -->

I think that the best way to approach this thread will be by splitting into sections. This will allow each section to be explained in more detailed. However, all of t sections will be based on the initial post that all of us that had submitted.

Local individuals: We believe that this will cause the most issue as most people value their privacy the most. Hence, all of us believe that there has to be an option for users to allow the software to use their images and videos and allow other users to search upon it. However, I was the only one that believe in collecting all the users' informations including images and videos regardless on the option that the user chose. This is to allow the law enforcement, who will need to have a warrant, to use our database to search for criminals or people they feel that needed to be tracked down easily. My partners believe that if the user has chosen not to share their data with the company, our software are require to oblige to their choice and not to be saved into our database. However, i we look upon Social Contract Theory, I believe that if a law enforcement agency have a warrant to search a person, it may create our society to be a safer pla Hence, it will be ethical for saving all the data from the user despite their option in using and saving their images and videos.

Local organizations: We will be buying data from other agencies that do collect and store webcam history as well as surveillance camera. This is to make our software to be better and more accurate when searching for a person than other software or company. As mentioned in local individuals section, by using Social Contract Theory, if we are able to make our society to be a safer place, this is ethical for us to buy data from other agencies.

Local society: To be clear, local society in my context is America. This is because I personally this that this will be affected in every part of any city or state. I believe that having this software implemented in webcam or surveillance camera can be beneficial as well as hurting people. It is beneficial as it may allow users to find out more about other users without asking many questions. All they will need is for the system to match their identity from the software or people's name for faster response. However, this hurt as well since it is capable of how people interact with each other. No information will be hidden from one another they have opted to share their data to other users. Hence, it can be ethical or unethical from Act Utilitarianism depending on each person perspective.

Global[1] individuals: If the person is a criminal and they are trying to flee the country, it will be more difficult for them. Since there are cameras installed in airport or ports, law enforcement are able to react faster and catch the criminal which will make the other individuals to be safer faster.

Global organizations: We will also buy data from companies outside America to allow better facial recognition and help the law enforcement to catch or track criminals.

Global society: I believe that all countries will prefer to be safe than in a country to be surrounded with many criminals. Hence, with our software, buying data from other agencies around the globe, and cooperation with law enforcement, it could be achieve. By using Rule Utilitarianism, everyone will be happier when

1. **Global**
Global issues in general equated to terrorism and keeping local country safe, which is a rather myopic view. How does it affect other countries such as in their economy, securty/intelligence, etc.? *[ananth]*

the world is filled with less criminal. Hence, it will be ethical.

Anonymous 2733
04/10/2014 11:39 PM

Since we were all sitting next to each other, and giving input, when you made this it's kind of hard to poke holes in it lol.

I guess I would just say that I agree with what was posted, nice job Michael.

As it's been stated in other posts I think yes it would be best to keep everyone's data in our database and simply not use it unless there's a court order.

And something worth mentioning about our global society and everyone being happier because the world is filled with less crime, is that it probably wouldn't lower the amount of crime kind of like the issue in England, however it would make it incredibly easier to catch someone after they've done it.

Anonymous 2718
04/10/2014 08:21 PM

Professional, ethical, legal, and social issues and responsibilities

Professional:

Addressing the list of fundamental principles gives some guidance on what some of our policies should be. The following three principles are most relevant tc the creation of our privacy policy:
1) Be Impartial – By making our system opt-in we would be impartial, not putting the good of our company above the good of the public. Additionally requiring law enforcement and government agencies to issue a warrant to use out software for solving crimes, also protects the good of the public.
2) Disclose Information Others Ought to Know – We can uphold this principle simply by presenting a readable version of our policy. By making it so that the average American can read our policy statement then they will have all the information they ought to know.
3) Respect the Rights of Others – By allowing people to opt-in to our service we can protect their right to privacy. We must also consider how to handle peopl who do not wish to be identified by the software and cameras with views of private properties.

Ethical:

One ethical issue is what we show people making a request on our system. If we allow them access to private camera feeds, it may be viewed as some as ai invasion of privacy if their face is seen despite the fact they have not opt-ed in to our system. One possible solution to this would be to only provide a list of wh and where a person queried has been, but then this would make verification by the user more difficult. If they cannot see the picture then they cannot tell for certain if that person was really there and this could lead to some possible false identifications.
I think that we all agree that there are certain precautions we must take when writing our privacy policy to ensure that it is ethical. First of all, we should make c policy easy to read, or at least have a shorthand version of the policy that everyone can read. To provide people with a policy they don't understand could be seen through a Kantian as not treating them as rational beings. A Kantian analysis also leads to an unethical conclusion if we use an opt-out policy. By not allowing people to choose whether or not they can be searched in our software, we would be treating them as ends to a mean; we would be using their identit and infringing on their privacy to make our software more marketable.

Legal:

Legally it is our responsibility to protect the rights of our customers and those who choose not to use our software alike. This means that we need to have sufficient security measures to keep people from accessing our databases without cause. Additionally we need to devise a way to reduce the number of false identifications to help those who do not wish to be recognized by the software. In this same area we need a way to prevent people from creating profiles for others, Justin's idea of somehow linking the opt-in with DMV photos is one avenue that we should explore. We should also provide a way for people to report false identifications in order to improve our technology and respect the rights of the people who have been falsely identified.
We all seem to agree that as far as law enforcement is concerned, police should issue warrants before being allowed to use private camera feed on our syste in investigations. This will be a large comfort to the public as we are protecting their privacy.

Social:

Taking a look at social contract theory, it seems very clear that we need to use an opt-in policy. It is unethical to hold the general public to a contract that they have not agreed to. As far as responsibilities are concerned, there are certain members of society that we need to protect. Obviously children should be protected and we should keep them from being entered into our system. Additionally people in witness protection should be protected from searches in our system as well.

Anonymous 2715
04/10/2014 10:22 PM

I would argue that it is ethical for the law enforcement to get access from the private camera feeds if they have a warrant. There should be a good reason why they have a warrant for those people in question. Through Rule utilitarianism, it will be ethical if the law enforcement is making good use and a good cause for the society. I will allow law enforcement agency to use my information even if I opt-ed out if they can make the society better which is safer environment.
Other than ethical portion, I agree with you in the other sections.

[no notes on this page]

Anonymous 2733
04/10/2014 11:33 PM

Well then the issue arises about the cops using a warrant under false pretenses. What if a missing persons report is filed and the cops get a warrant to search the person on our database, and it turns out that that person, who wasn't opted in, gets tracked down and they simply wanted to leave without saying anything? Seems like that persons' privacy would be violated even with the police getting a warrant.

Anonymous 2733
04/17/2014 04:14 PM

.:*Policy Statement*:.

Anonymous 2733
04/17/2014 04:24 PM

So, Alex and Michael, we all agree that law enforcement agencies are gonna need warrants to get access to use our service if it includes private camera feeds. Should this be the only thing they need a warrant for or should we be more strict?

I'm thinking we've generally agreed to keep our product restricted to the United States.

It would be an opt in system.

We would store a person's information even if they aren't opted-in and only access it under a warrant.

We would be willing to buy and sell camera feeds from companies.

We would be willing to sell our service to the public.

We would do our best to make a clear and easily readable terms and conditions policy.

Anonymous 2715
04/17/2014 04:48 PM

In addition, I would also add that the policy would state more information about the person information even if they are not opted-in. In other words, not only that we would state that we would store a person's information even if they aren't opted-in and only access it under a warrant, as mentioned by Justin, we should also elaborate on why we would do that and explain the necessity of doing so in our policy statement.

Should we also include that users have to pay or advertised while using the software? I believe that this should be written in our policy statement as well since we would want users to know about our policy and be clear to them that either they have to pay a fee, fill the software with advertisement or something else. The users ought to know.

Anonymous 2718
04/17/2014 04:49 PM

Justin, what do you mean by "more strict," if law enforcement serves us a warrant there is likely little we can do in the way of preventing them from using the software in ways outlined by the warrant.

Would we really want to store a person's information even if they haven't opted-in? If this information became available to the public, there may be some uproar about invading their privacy. What if our servers got hacked? Then these people would have their information out there even though the chose not to use our software. I think in the case of a warrant, we could add the person as if they were a new user which would protect the rights of those who chose not to use our software.

Additionally, I think we need to include in our privacy policy how we will collect pictures to use for facial recognition matches - Justin's idea of somehow linking a user's account to their driver's license seems like a good idea.

We also need to determine what other data we want from a user and how we will use this data.

We also need to come up with policies regarding kids, and public spaces that we would not take camera images from.

Anonymous 2733
04/17/2014 05:08 PM

By more strict, I meant what would we supply willingly without a warrant. However later I say we would sell it to the public, so agencies could use it that way. The only thing I can foresee the government needing a warrant for is using a warrant to use our software on someone that isn't opted-in.

As for the paid service versus free service with advertisements, I personally think we should do a paid service because our software seems kind of limited in number of users. The add revenue works well for companies with a ton of traffic like google, however doing a webcam timeline search seems like more of a targeted service that might not generate so much traffic.

[no notes on this page]

Anonymous 2715
04/17/2014 05:19 PM

I agree with Alex as she brought up a good point. I have not thought about what would happen if someone broke into the software's database. My opinion would be that we would have a policy statement mentioning that if our database does get leaked or stolen. However, should we tell the users about it or should we just state that we are not held responsible or how should we handle it?

My personal take is that the company would not held responsible as I believe that it is not within our power to fully prevent of such happening to us. The company would try its best to protect the database from being leaked or stolen, but not fully prevent it.

Anonymous 2718
04/17/2014 06:13 PM

I agree with Micheal, that we should include a point about leaked/stolen information in our privacy statement, however the point I was trying to make is that this is a reason why we should not store data for people who haven't opted-in to our services.

I also agree with Justin's point that this needs to be a paid service. There probably not enough demand for us to profit from advertising rates alone. Speaking of making profit, will we sell any of our customer's information or location data to other companies? While we do allow members of the public to use our services, will we let it be used for corporate use? If we are willing to sell camera feeds to other companies are we willing to sell the information of who is on those feeds with them?

Anonymous 2733
04/17/2014 09:20 PM

I think it's reasonable to sell our product to other companies, especially to department stores so they can play adds that will relate to the individual and potentially benefit everybody.

The way I was thinking our system would work is we would save all our footage for maybe the past 30 days, and we would build profiles and timelines as things occurred for those who are opted-in. For those who were not opted-in we would still have the footage of them but no profile would be updated and no notation of who they are would be put into our system. Now when a law enforcement agency shows up with a warrant asking about a specific person we could put that persons picture into our system and it would build a profile of that person using the footage we have stored of the last 30 days.

As for database being compromised I think that obviously we need to do everything in our power to prevent such a thing from occurring. Whether or not we would be held responsible if it was compromised isn't really pertinent in this scenario however.

Pertaining to the kids concern, this is an opt-in system and parents could opt their kids in. Also in the case of kidnappings, or run-away minors, a warrant could be issued to track them down.

Anonymous 2718
04/17/2014 09:44 PM

If you look at the assignment, it says that our system will be able to search and keep track of people at locations from several years. If we only keep footage for 30 days, if someone makes a request like the ones in the assignment ("Where was John Doe at 5 p.m. on March 15, 2008?," or "Who was at the Washington Monument at 6:33 p.m. on January 3, 2010?") users who have added themselves to our database after those dates will not have that information updated meaning that our lists will be incomplete.

How will we verify that it's a child's parents signing them up for use of the software? What measures are we going to take to reduce the ability for people to sign up others without consent?
And if we allowed kids to be opted-in would we set it up to limit the people who can search for them to further protect their privacy? Facebook and other social media require that you be at least 13, and often set limitations on how youths can use their services to protect them.

Anonymous 2715
04/17/2014 10:48 PM

If this software is a paid service, will it be a monthly service or one-time payment? My personal take is to allow to have both option. If the user choose the monthly option, I think we should notify the user our policy again regardless if it is updated or not whenever the user have to renew, else if the user chose one-time payment, the user will get a notification by either email or from the software that there is a policy update. I also think that within our policy we should mention that we are allowed to change our policy without notification.

My take upon users who are not adult should not be able to create an account unless their parents created one for them. Since, it is created by the parents, it will have parental control. Hence, within our policy, it would mention that the company would not held reliable if their parents created one for their children.

I still believe that our policy of storing data should be what Justin mentioned previously, which is storing data regardless of the option that a user chose. Since we are trying to help law enforcement, we should store the data. However, law enforcement do require a warrant before accessing the data from our database.

Anonymous 2715
04/17/2014 11:01 PM

[no notes on this page]

I have some thoughts on how to prevent kids from using the software. I believe that if they are kids, they would need an additional step for them to log on to the system. The additional step is using the software main purpose which is facial recognition. If they fail in the facial recognition which is set by their parents, they would not be granted access to the software. I think this could deter kids from using this software without their parents consent.

My conclusion from this thread is that we believe we would post every policy that a user needs to know before using our software. This is the list that I believe summarize this thread in addition to what Justin mentioned in his first post.

Kids who are not adult(below 18) would require some consent by their parents.

Company would not held responsible if there is a leaked or stolen database occurred.

Data are stored for a long period of time for users who want to search upon people.

[no notes on this page]

Team Project Discussion - Team 10

Toggle Anonymity

Select Discussion: Team 10

Please see attached prompt and rubric.

Enter new discussion post here...

Post

Anonymous 2737
04/03/2014 09:41 PM

Team Discussion for Team Project:

Introduction:
The scenario we are presented with is hypothetically if we start a company that develop "webcam history" technologies. With the best facial recognition technology this new product is able to process surveillance cameras and find people that are in the videos. Basically as a team we are suppose to come up with a guide line for ethical use of this newly developed technology.

Personal Take on Ethical Data Gathering:
Obviously this technology should have access to the public agencies that are available online given that our new technology gets the permission to do so. For the public agencies that are only used by law enforcements the data should be separated into two categories. One categorize is for law enforcement usage o as in no one else that use this new technology will have access to these data at all. Another categories is to give these public agencies a choice of making these data available for public usage or not at all and maybe for a compensation or with an agreement. And lastly for the private agencies they have to choice not supplying data or to supply data and have the control of who can access it or not. The private agencies can even lock law enforcement out of this data set unless required by U.S. law to do other wise.

Users' Personal Information:
For this section I think it is reasonable to divide the situation into 3 scenarios. First one is data being used by the law enforcement agencies. The law enforcement agencies already have a database of a bunch of people in the U.S. so it is ethical for them to use the webcam history technology with their own database of picture, names, etc. when there is proper cause of course. The second scenario is for the use of public. For this usage it is best for a opt-in polici where people make accounts in order to be opt-in into the database. For the account the user control what kind of information is associated with the account like birthday, interests, place of employment etc. The basic information needed for an account would be name and social security number, the SSN is not stor but is used to verify the identity of the account. These accounts should also give the choice of being available to everyone, to public agencies, or to private companies. The last scenario is for businesses and companies that use this technology by either licensing or other means. Like I said above the average use should have the choice of being opt-in for these organizations or not and what information is available to whom.

Access to the Technology:
The users will have to read the policies and agree to the things I've mentioned above in order to have access this technology and by breaking the rules they ca be sued or prosecuted as an illegal offense depending on the action of the user. I think the users' that are opt-in to this technology should have control of their own history. The users should be able to delete certain part of the history if they don't want it associated with their profile or make some it private and some public etc. Any data that is not public should be exempted from being sold, disseminated. It is acceptable to be collected but our company should not have the right to access it just like emails in gmail. Buying and selling of webcam history data is acceptable if the person which the data is associated to agrees to it. This is useful for things like making documentaries, record keeping etc. Lastly the technology can be available in multiple countries but the policies between each country is going to be very different depending on what country it is. Also the data collected from different country should be separated unless the user chooses their data to be available internationally.

Conclusion:
These are some of my initial thoughts, you are more than welcome to give me feed back or ask question.

Anonymous 2726
04/09/2014 05:13 PM

I love the way you have split the access of the technology into multiple avenues, those that are for law enforcement, and those that are available to the general public.

Also, it is interesting to allow people to be able to edit their past histories to change what is publicly available and what is not. I do not think they should be able to delete any of their history seeing how they might be deleting something that they did illicitly.

Anonymous 2724
04/10/2014 06:07 PM

I like the way you stated your rules for usage, however terms and conditions are probably not the way to go about it. While they are good for legal

1. **Obviously this technology...**
Sloppy writing makes it hard to read. *[hauser]*

2. **The users should be able...**
good point. Didn't see this raised in other case studies. *[ananth]*

reasons people tend to not read them.
With the idea of requiring account information, I Agree, however I would also suggest that a small fee be transferred. While it would be more or less superficial, the point is that if an actual sum of money is exchanged the legal specifications become much clearer. Also if people have to pay a small fee they are more likely to read everything they need to.

Anonymous 2724
04/03/2014 11:07 PM

So, obviously this topic hinges on the idea of privacy. Cameras of this sort are used in other countries (I believe Britain has a CCTV system for instance) and while those are used for security measures they could easily be used for private matters. Such as finding if your partner is cheating, or where your child is goir and not telling you. For the sake of argument I'm going to separate it into two groups, gathering the info and accessing it. Although storage is also a factor in t case, that falls into the accessing part as it doesn't do anything unless you use (access) it.
Gathering the information seems to be the easier factor here, as we are only hooking into systems that are already available. We are contracting the usage o specific technologies and filtering them through our central system. However we do have an ethical responsibility with this information, for instance attempting cross reference it with sites such as Facebook. Compiling this information may be a breach of both the site and users rights to privacy and may not be acting the best interest of the general public (Code of ethics). However compiling this information may help improve the service, say you discover through data minir that the person frequents Chinese food. Now it cross references your Facebook calender, and suggests that you check out a Chinese place, and even has good times where the place is not too busy. The store could even market that it as a deal at specific times to the service, meaning metrics for when the store i empty could be used to try to improve the number of customers over that gap. However this is a massive amount of data, the number of people in a store, storing where you are and when. It is also a serious case of invasion of privacy and its impossible to ask each person if its ok, massive case of treating peopl like irrational beings (Khant).
With this it is easy to say that you will have it be opt in, however this only works as long as people do not attempt to impersonate each other. If they opt in unde another persons name they would quickly get that person's public information (This ties into accessing information, however it is more related to starting to gather the specific information) from there someone could stalk people with very close accuracy, the person would not be able to escape the network of cameras that this person is finding them with. To prevent this it would be required that the person submit either paperwork and a verified ID to be opted in, an be able to opt out at any time. It would also be a good idea to prevent specific people from being included in the database, such as people who either reques to be permanently blacklisted, or people who were recently involved in large scale criminal cases. While this last point seems random, it would prevent peopl from getting access to suspects or victims, it would also allow victims time to fix themselves to the permanent blacklist if the crime may have lifetime implications. As an extension of this though, any warrants would trump this. Even though we are not storing a person's specific information law enforcement (provided they have a court order) can force opt-in people to a private context (law enforcement only) This way while khant says we are not treating the persor rationally, the good of the general public is served by getting the witness or catching the suspect.
As for accessing information, this is nearly impossible to regulate. With having government only you have a very limited marketplace, and are unable to sell to consumers (the main audience). For this reason any policies will need to be buried in mountains of legalese, there are too many ways people can lash out an sue because of a system like this (for instance guy sues because his wife left him because she saw he was cheating via the service). While this is very underhanded, it is required to maximize the stability of the company, this prevents the need to sell more information to cover legal damages and reduces the amount of advertising revenue required to run the service. This means less companies receiving the information and a much more rigid vetting system for tho companies can be established.
With webcams, I do not think we should include them unless the person specifically requests and opts in to webcams. There is an assumption of privacy with them.
Also_multiple_countries_introduce_issues_with_cross_boarder_legality{comma}_some_governments_may_abuse_the_system_and_even_our_own_possi _will.

Sorry_for_underscores{comma}_only_way_to_have_more_than_750_words{period}_Also_punctuation_counts_as_word_ends.[1]

Anonymous 2737
04/09/2014 10:06 PM

I like your take on certain people can access it and certain ones can be denied access due to their actions in life. Since this would be a service denying people from using it is not a infringement of any bodies rights. I don't really think being sued would be an issue since an opt-in approach is taken. If a guy gets caught cheating first he has had to be opt-in in order for him to show up in the database. So if he is opt-in then he is agreed to some sort of user usage agreement and so by law they can't sue. Impersonation could be an issue which is why i suggested that working with the government to identify people for this service is necessary with the usage of SSN or other type of identification.

Anonymous 2735
04/04/2014 04:19 PM

Technology that is as invasive such that locations and activities should be carefully handled. The ethical issues that arise because of this technology mainly include invasion of privacy that could possibly lead to a big brother type scenario where a government, or company, or a person knows what you do at every moment. Looking at this issue the biggest concern is privacy and what right citizens have to it depending on their location. For example it is perfectly fine to ta pictures of people at a public place like the Washington Monument, so in an ethical framework like social contract theory the proposed technology would not have any issues. But if you look at this situation through most other ethical frameworks, like kantianism or act utilitarianism this idea of monitoring people through cameras and facial recognition may be unethical depending on how you operate it. As such many protections for people's privacy must be taken into consideration, as well as the intended use of this new technology before it is distributed in order to appease all concerns that this technology may bring up.

To begin, what should be collected from the user, and what would the intended use of this information be? In the example listed, the time, location, and persor name can all be found, or if you just searched a location and time you could find a list of people who were at that location. For public use this would be a disgustingly large amount of information to be able to search for. This technology could be useful for law enforcement, if a warrant was given to search for suc information, but in terms of other government, or private use the information listed is too much. The first remedy to this situation is to make signs which show t this area is being recorded and is using this high-tech facial recognition software so people may at least be informed of the areas that it is in use. Second an opt-in policy would be necessary such that only people who opt-in may be found using this facial recognition software such that people who wish not to be fou will not have to simply avoid areas in which this technology is used.

With an opt-in policy users who allow themselves to be found with this technology should then allow how they can be searched, i.e. if this was integrated into a

1. **Sorry_for_underscores{comma}_only_way_to_have_more_than_750_words{period}_Also_punctuation_counts_as_word_ends....** innovative! *[ananth]*

social media site they could then allow their friends to see what they have been up to; or if they go full throttle they could allow anyone to see their activities, an thus allow for companies to search their information to do targeted advertisements or offers. Because this technology is so invasive though, a user should be thoroughly informed of exactly how this technology works and how others are able to use it, as well providing an agreement for the user to read over before the opt-in such that what they agree to is documented.

The opt-in and use mentioned in here are very basic and would need to be expanded upon but the general idea is to only allow informed users to use this new technology and decide how they use it, whether to form a mutual relationship to companies, or to up to date communication happens with friends on a social media site.

Anonymous 2726
04/09/2014 05:27 PM

While reading through your post I started thinking about a discussion I was having recently, it was about the recent mandate[1] that all new cars must have cameras in them by 2016. The discussion was about how by 2016 or 2018 all new cars were to be required to have a camera facing every direction and I was thinking, what if these cameras were hooked up to a wireless internet connection that tried to connect to all the free wifi access points around it and these cameras were also used... After doing some research I could only find some articles about all new vehicles being required to have rear facing cameras by 2016 or 2018 in order to facilitate safer backing. But, still, being able to utilize all those mobile cameras would be phenomenal for this technology.

Anonymous 2724
04/10/2014 06:14 PM

I like your idea of having the opt in facial recognition, and your idea with the signs gave me an idea. While the signs are probably not the best, it would be expensive to put the up, and it would require specific equipment to prevent recording outside of them. My idea (I presented this in class a while ago, and was somewhat laughed at but oh well) is that people use some sort of ID app on their phone or a token of some kind (Something similar to blizzard's authenticator). With this it would only search for faces of the people who have opted in locally, and who have that device. This would also lessen server load as you have a local list of faces to check against.

Anonymous 2726
04/09/2014 05:08 PM

First off, the notion of this technology scares the crap out of me.[2] I think it would be crazy if you could go to a website, type in someone's name, give the compa twenty bucks, and then suddenly know the general whereabouts of a person for the past few months, years, or decades. I mean, it is an awesome idea and it would be a very powerful technology. But, it almost seems like it would be too powerful.

Addressing what personal information is to be collected from the user and why, I think this should be held to a minimum. A picture of the user linked to their name should be plenty. If this information was expanded to anything further I do not see how it would be useful to the purposes that this technology is suppose to supply. If it is a governmental agency looking the person's locations up, they can get other information through their other sources. If it is a private business private party looking up an individual then they have no business getting anything more then their name.

I am not sure how an opt-in, opt-out methodology would work with something like this. It almost seems like the idea is to be able to track everyone and if someone can just opt-out because they feel like it then the system would not work.

If the only thing we hold on our databases our people's names and pictures then the necessity for extremely good security might be at a minimum. But, if we a also holding onto the records of where all those people have been at any given point, then the security would have to be phenomenal in order to protect those individuals as well as our investment into the information that we have gathered as to the whereabouts of all those individuals.

Nothing would be made available to law enforcement without a court order.

Their picture is the only thing used to profile them. Only their appearance.

The only thing that could be sold to third party vendors would be the whereabouts of individuals that they pay for individually.

I think that the webcam histories that we have access to would be completely exempted from being revealed except by court order. I think this would be the be way to keep the information we have secure and relevant to any potential customers that we would like to reach.

We would most definitely try to purchase as much webcam history data from other companies as we could so that our database would be more complete and would have the most complete picture of the world that we possibly could. On that note, I think that this should be as worldwide as it possibly could be, that wa our profits would be the highest they possibly could be and we could provide the most complete picture of someone's travels and locations as we possibly co to the customers that would be keeping our business alive.

I think that the ethical framework that most fits my train of thought would be that of Rule Utilitarianism and the universal rule to be applied would be that a company should maximize their profits while protecting the privacy of individuals as much as they possibly can.

Anonymous 2737
04/09/2014 10:00 PM

I feel like you are looking at the extremes here. The data we can gather from this technology is not as powerful as you make it sound. Think about the places that actually have 24 hour security cameras, then subtract the places that are not participating. Unless there is a sudden new trend of security camera everywhere then this can be powerful but right now the amount of security cameras is really not very high. I think the data this technology can gather would be a snippet of someone's life at very public places which is not information that extremely important.

Anonymous 2724

1. **the recent mandate** some evidence of lifelong learning? *[ananth]*

2. **crap out of me.** Colloquial. *[ananth]*

04/10/2014 06:21 PM

I agree with Jiurong, I do not think this is as observing as you seem to think it is. If you were to get a persons whereabouts, it would end up being very general information, or information of where you are in public places. People may be able to gleam where you went for vacation, however they are not going to get your private life. They only get what you do I'm public, where it's public.

Anonymous 2726
04/10/2014 08:33 PM

But it's not normally accessible. For someone to know where you were, what you were doing, etc. they would have to actually see you. With this technology they could just type your name into the database and know. Just like that.

I also feel like as soon as there is a technology like this whoever controlled it would start putting cameras everywhere with all the money they would be making.

Anonymous 2735
04/10/2014 04:20 PM

o Professional, ethical, legal, and social issues and responsibilities. In this thread, engage in a discussion to identify professional, ethical, legal, and social dimensions of each proposed decision or policy. The ethical frameworks and Code of Ethics discussed in the class must be enlisted to provide a rationale fo and/or against each proposed decision or policy. In cases where competing ethical perspectives or Code clauses are in conflict, the team should attempt to resolve the conflict by prioritizing competing perspectives/clauses and/or using its best judgment.

Anonymous 2726
04/10/2014 08:45 PM

1

I feel like the only article of the code of ethics that this technology would be breaking is 1.7 which says that, we will respect the privacy of others. This is encroaching on people's privacy. Even though it will mostly be recording people in public areas I still think it is a violation of privacy for anyone to be able to look up someone's name and get a log of all the locations they have been spotted at.

Anonymous 2735
04/10/2014 09:06 PM

There is also the potential of this new technology breaking the first principle of the code of ethics which states "Software engineers shall act consistently with the public interest." Though we can't anticipate at this point how the public feel about this new technology being implemented.

Anonymous 2724
04/10/2014 10:00 PM

On the notion of this being a violation of privacy, this company is not to make new programs, it is only to identify people through them. So while we would be exacerbating the violation I do not feel we are the source of it.
While many frameworks would find it unethical to take the pictures, we need to focus on that we are only sorting through them. Through this frameworks such as kant and social contract theory will depend heavily on how we handle the inclusion systems.

Anonymous 2737
04/16/2014 09:39 PM

Yeah I agree with Daniel the data is already there we are just looking through them in a fast and efficient way we can talk about whether the collection of the data is in violation of privacy but our program is not responsible for the data that is already collected. Also with the opt-in approach people that does not want to be included in this service is protected only people that agree to being put in data base would this system locate which they all agreed to when signing up.

Anonymous 2735
04/10/2014 04:21 PM

o Local and global impacts on individuals, organizations, and society. In this thread, engage in a discussion that explicitly considers the local and global impa of each proposed decision or action on key stakeholders, including individuals, organizations, and society. In addition, assess the certainty with which you ca determine the impacts of each proposed decision or action.

Anonymous 2735
04/10/2014 05:53 PM

One of the biggest impacts this would have on individuals and society would be that anywhere they go they have the potential to be monitored. Though this may not be as scary as it initially sounds since most places have surveillance cameras already, and this would just further the technology into full on recognition of a person. Also most people don't even recognize the many times they are being watched so adding this new technology the general society may be just as ignorant of it.

Locally this new technology would have the potential to decrease crime rates. In towns or cities this technology may also be applicable to the local governments in finding statistics on what type of person likes to do a certain activity, to further target and enhance town/city funded events or to find

1. This is very interesting that they think that the code of ethics is something to be concerned about if it is being "broken" rather than something that should help guide decision making in situations that are complicated and nuanced. *[hauser]*

what markets might thrive in and boost their towns economy.

Globally the same things that might be applicable in the smaller local setting would just be furthered. It would allow organizations or companies to find out what certain demographics like to do, and how to target them. This type of more personal information that has the possibility to clump large chunks of people into one group could definitely change the interaction people individuals and organizations thus changing society as a whole, thought he change may not be noticeable.

Anonymous 2726
04/10/2014 09:37 PM

It's been shown that surveillance cameras have nearly zero effect on the prevention of crime. They just make it easier to figure out who did it. I don't see how this technology would serve as further deterrent to criminals. If they're going to commit a crime, this probably isn't going to stop them.

Anonymous 2724
04/10/2014 10:32 PM

There are quite a few stakeholders in this situation, the largest groups being other companies, and the public.
Other companies would get more information on people's actions, find better marketing strategies and such. This may also be a positive for the public, as it would allow people who want specific products to possibly find them easier.
The public is much less black and white though, this information can have both positive and negative effects. It is more a matter of how imaginative you are to find situations for either. As examples a positive could be you somehow lost your vacation photos, however because of stalker tek programming you have all of them at strange and awkward angles. A negative would be someone impersonating someone else in order to find and harm them.

Anonymous 2737
04/16/2014 09:58 PM

I think there are 3 stakeholders, public, companies and the government. For the public the effect is about even this technology might lead to finding criminals faster but at the same time for criminals to find it's victims. For the companies I see no downside from this technology and there are various ways for them to benefit. For the government it might be cheaper to find criminals and at the same time more crime might be caused by this technology.

Anonymous 2726
04/10/2014 05:38 PM

o Further knowledge and research needed. In this thread, engage in a discussion that identifies additional knowledge (facts, laws, statistics, etc.) that you nee to know in order to make the best possible decisions or choose the best possible policies. Fill in the gaps you identify by performing research to seek and evaluate outside sources, making sure to cite each source. In cases where you choose not to perform additional research, identify appropriate methods you would use to obtain the information.

Anonymous 2735
04/10/2014 09:13 PM

Further knowledge we would need to know is how far reaching this technology will go, just within the United States, or will this technology go international. If this technology does develop past the United States we would have to make sure we take into regards those countries laws. It would be a pain in the ass to research every countries privacy laws at this moment, but it is simple to look up the subject for any relevant countries.

Anonymous 2726
04/10/2014 09:33 PM

The way we could obtain that information would be by contacting our legal department and asking.

Anonymous 2724
04/10/2014 10:04 PM

As some of our topics were based on Britain's CCTV, we should probably research why their system was not effective in preventing crime and what systems they had in place.

Anonymous 2737
04/16/2014 09:51 PM

Well if you think about the quality of most security cameras and the accuracy of facial recognition technology (Think about hats, sunglasses, hoodies) That is probably why the Britain's CCTV was not successful. Like i said this technology would be using a massive amount of data collected but the practical usage of these data is very limited.

Anonymous 2726
04/10/2014 05:39 PM

[no notes on this page]

o Biases and assumptions. In this thread, engage in a discussion to identify and analyze your personal biases and assumptions about the scenario. These biases and assumptions will be important to make explicit as you move toward identifying viable approaches and courses of action.

Anonymous 2735
04/10/2014 06:15 PM

For biases, I definitely have a bias since I don't entirely believe this technology with the way it can identify and track anyone is a good idea. I think that this technology would be a very poor idea without some heavy censorship as to what type of data gets through. I also don't necessarily know if with enough changes to privacy policy and the way the technology is used my opinion will change.

For assumptions, for now I will assume that this technology will not be changing or developed further past using facial recognition in order to identify a person, and to see the places people have been to, or the people who have visited a place.

Anonymous 2726
04/10/2014 09:08 PM

I think my bias against this is mostly that I am terrified about the potential of this technology. It could be used for so much bad, so much so that I think it greatly outweighs the bad. I guess the assumption I am making is that this technology would not be able to have enough safeguards on it to ensure peoples safety.

Anonymous 2724
04/10/2014 09:55 PM

My bias is what is the fear of it. If everyone has access to this information then it may be shocking at first, however it would quickly change to be the norm. It would become a more open society. If that's good or bad is anyone's game though.

Anonymous 2724
04/10/2014 10:02 PM

I would just like to ask the question, it seems like many of us are afraid of this technology. But what exactly about it are we afraid of and why?

Anonymous 2737
04/16/2014 09:47 PM

My bias is that this technology would not be dangerous since first of all it does not track people because there are not that many cameras around and the data this technology collects are bits and pieces. Secondly the only people that can be tracked are the people who provides a clear picture for facial recognition. Lastly this is kind of like the NSA where they can collect massive amount of data but the practical usage of the massive data is limited and labor consuming.

Anonymous 2726
04/17/2014 01:49 PM

I'm afraid of how accessible the information would become. As of right now, it is rather difficult to track and locate an individual. With this technology, as it was described, you can type in someone's name and get a snapshot of the past few months, or so, and know exactly where they've been spotted. That is what is frightening. The ease that someone would be able to look it up.

Anonymous 2737
04/17/2014 07:15 PM

Policy Statement Thread. Start a new thread entitled “Policy Statement,” and use the thread to converge as a team upon a set of decisions and policies to address the scenario.

Anonymous 2737
04/17/2014 07:22 PM

The few policy we should have is first we need to have the data collection policy where it is an opt-in policy for private security cameras and contracts with the government for public security camera data. Another policy is the user opt-in policy where they provide name and maybe ssn for identification but ssn is not kept in the database and any other information the user would like to provide. Lastly we need to address the access policy where people who have criminal records should not be able to access and users need to make an account so there is accountability for data access.

Anonymous 2726
04/17/2014 09:53 PM

As for governmental and police force access I believe they should be required to have an arrest warrant to look up someone's whereabouts.

Anonymous 2724
04/17/2014 09:58 PM

[no notes on this page]

It should also be a thing that a person gets a notification for when they are looked up, and probably has to accept that the person gets their information (accept in the case of law enforcement) This would be intrusive though, so any other thoughts would be nice.

Anonymous 2726
04/17/2014 10:03 PM

Well, first the opt in dealy, and then they can have multiple settings where they can either have it open so anyone can look them up, closed so no one can, or somewhere in between with a myriad of notification settings.

They could be open and notified, open and not notified, only friends and notified or un-notified, friends and friends of friends with both notification options, or on an approval basis where they get a notification seeking approval for the look-up.

Anonymous 2735
04/17/2014 10:37 PM

Another issue is how long would this information be stored, one year or two years or even indefinitely? I believe that one to two years would be a suitable storage time for this technology.

Anonymous 2735
04/17/2014 10:40 PM

Also how do you feel about obtaining a warrant every person who visited a place at a certain time? While it would be reasonable to get a warrant for a single person what if the police conduct a broad search by wanting to gather information on anyone who went to a public place with this system installed.

[no notes on this page]

Team Project Discussion - Team 05

Toggle Anonymity

Select Discussion: Team 05

Please see attached prompt and rubric.

Enter new discussion post here...

Post

Anonymous 2719
04/03/2014 12:43 PM [1]

It is very important for us to have an Opt-in policy to ensure that we protect the privacy of our users. No user should be tracked and have their actions documented without knowing and without first giving us their consent. By tracking people without them knowing or agreeing we would be using them as a mea to an end for our business to gain profit. We would not be following the fundamental principle of Being Impartial, by monitoring people without their consent ou company would be promoting our own gain at the expense of society, we are also respecting the rights of others.
We must put high importance on having strong contracts with law enforcement agencies, so that we can stop crime in public places. We do not need to identi who the individuals are in the footage to know that a crime is taking place and to have the police send a squad car down to protect the innocent. By having a strong tie with the law enforcement we are disclosing information that others ought to know while maintaining our integrity by not identifying who is in the video feed if they have not opted in.
The information held by our system will only be data that is considered public knowledge, to protect the privacy of our users we will also allow them to go in an omit any information they feel should not be shared with the public through our services. Due to the chance of impersonation, users will not be able to add information that they deem necessary for others to know over the computer, but this is possible if a face to face meeting has been set in place.
All users who have and account and have opted in to our services will be able to search public locations and these locations will identify people your account has identified as a friend of yours. To become a friend both accounts must mutually agree to allow the other to identify them. Ordinary users will not be able to search for specific people, unless that person is in their immediate family and is under the age of 13 years old. In the case of a missing person Law enforcement will be able to search for a specific user, if that user has registered with our system prior to the search in order to disclose information that peopl ought to know and to also protect privacy. If an agency disobeys our policy and searches for someone using our system without first getting our approval, that agency will no longer have a contract with us and will still have to pay the remaining elite subscription fee.[2]
The main goal of our company is to improve society while still treating everyone as an ends in themselves. The idea is to improve the quality of life for everyor by making people feel safe and also by providing simple information like what does the traffic look like on this camera or are any of my friends hanging out at the beach. If our product does not follow these two guidelines or if we fail to protect the privacy of others we will change it until it does, and if we do not succee we will discontinue our services indefinitely.

Anonymous 2732
04/10/2014 02:33 PM

One way to meet individuals' reasonable expectations is to separate the information that is considered public and private. Public information should not intrude on anyone's privacy rights, thus it can be more easily accessed.

Anonymous 2732
04/03/2014 08:00 PM

With the emergence of new technologies, we must consider how these innovations might ultimately change our behavior. The right to privacy that each persor can reasonably expect is one aspect of our lives that may be affected by these technological innovations. As more information is gathered about people, we must consider how this information can be used for better or worse and also how this information is accessed or distributed.[3]
In regards to the limitations of the personal information that we will gather, our services will gather only the data that is relevant to our purposes and nothing further. In addition to webcam history and locations of individuals, we will gather or infer information that may have some use for our clients. Our company will offer an opt-out policy[4] for any person who does not wish to be included. All of the information will be stored on a central database which will pose the highest standards of security in order to protect and preserve the sensitive data we will gather. In addition to the clients that we serve under contract, this information v be made readily available to law enforcement agencies who petition us with a warrant. Those who do not possess a warrant will not be given access to the entirety of our database, but rather will have access to the information that is considered to be public. In order to construct user profiles for the individuals monitored, we will gather data pertaining to the locations that each individual was identified. From this meta-data, we can infer simple patterns in their regular travel behavior. The frequency at which individuals visit certain locations may also serve as an important aspect of their profile. Third party vendors will not receive any of these data that is gathered directly from this company. Only our clients and customers with whom we have licensing agreements will have acce to this personal information. Note that we are not responsible for any information released by our clients, as specified in the licensing agreement.
In regards to the amount of access that our users will have to our technology and information, we will fulfill the terms with our clients, as specified in our licensir agreements. The policies by which our company will adhere to will be displayed with the utmost transparency and clarity. In order to provide the most extensiv service, contracts can be made to purchase web cam data from external entities. Any web cam data that has been shown to infringe upon the rights of any individual will not be collected, and any such data previously gathered will be omitted from the database. The data gathered will be made available for purcha

1. **Anonymous 2719 04/03/2014...**
This seems to throw together a bunch of words and phrases that the student has learned in class without showing much understanding of them and their implications. *[hauser]*

2. **treating everyone as an...**
I am not sure what this means. Must be a zen thing. *[ananth]*

3. **With the emergence of new...**
This is a good starting perspective. Let's see where it goes ... *[hauser]*

4. **opt-out policy**
interesting... *[hauser]*

by our clients, if and only if the information does not violate the rights of an individual and the client asserts that this information will not be used with any malicious intent. The technology that is used will be made available internationally, with the utmost respect to international law. We shall not violate any international treaties or sanctions in order to expand our technology. The laws of individual nations shall also be respected and these technologies will exist o were it is permitted.

Anonymous 2730
04/03/2014 08:42 PM

When thinking about this problem a key aspect to take into account is privacy. Due to the fact that facial recognition is not perfect, a person may be matched with a profile even if the picture is not of them. This goes against the clause to respect the rights to others from the code of ethics. This process would only wo if there was an opt-in option which let the person know clearly what information will be taken from them and will need to have some other form of identification besides the facial match for if the match is incorrect. The database should be very secure even if it only stores name, picture, location, date, and time these pieces of information are still sensitive and can be used against the person. Without a court order a government agency will only be able to look at people wit surveillance cameras that they control. The information used for user profiling would just be picture, name, location of camera, date and time. Information is or shared to third-party vendors for users that opt-in to get advertisements that pertain to where they go. By having the user permit sharing of their information makes the process ethical from a Kantian point of view because it is treating the users as rational beings. The policies would be very clear in bullet point form with as limited amount of text as possible. By making the policies clear the clause to disclose information that others should know as well as taking responsibility for companies' actions. This will allow users to make informed decision and will keep the website from getting backlash. As long as the information is only gained through legal means then no information is exempted from being collected. The webcam history data would be useful for law enforcement to see the history of a person that is on the run. The information would not be sold and webcam history would not be bought because it is not needed. This technology could be available in multiple countries, but this relies on the laws and such of that country. Creating a public website would not be a good fit for this kind of software. The only person that a user could look up would be themselves otherwise they would be violating privacy rights of others. Contracts would be setup for the use of security cameras with private agencies. The technology could be licensed to other companies so they are able to use within their companies to keep track of employees and such. The only way a public website could work would be if it did not include specific information on users except for location information that pointed out how many people visited an area at a given time keeping identities confidential. Even if a company does not know who is visiting their store they would be able to tell the times when there is the most traffic and when less employees are needed. The public website would only show public locations. The main issue with setting up a service like this is dealing with the error of facial recognition and making sure that people understand how and what the information will be used for.

Anonymous 2717
04/03/2014 11:48 PM

To implement this technology, there are many moral hurdles that must be overcome. Dealing with each person involved, unless there is a crime committed, there needs to be some sort of opt-in feature, otherwise identifying people based on this technology would be a huge invasion of privacy. The person using th technology would need to surrender a lot of personal information, otherwise it would be feasible for the user to use this technology to commit a crime themselves, by essentially allowing this technology to be used as a virtual staking machine. Going hand in hand with this, the database would need to be very secure, otherwise, as aforementioned, it could be used as a stalking machine, which would not end well. I feel like none of this should be available to Law Enforcement, unless a crime was committed, since they could use it to needlessly monitor people for no reason. As for what should be available for third party vendors, only locations that would promote commerce would be used for sales. For example, cameras at a McDonald's would be used to identify people and sell ads for food places, while cameras outside public places (parks, libraries, etc.) would be free of use, since they are public property.

The policies dealing with this would have to be clear, and the terms would have to be read before accepting them. It would be hard to enforce, but giving it a timer or forcing the user to print the terms would be sufficient to cover this requirement. I also feel that commercial cameras would be used for commercial purposes, while public cameras would have to be free to use, since it is a public property. Histories would be recorded, but only ever used in criminal investigations, where the crime was caught on film. Using histories for commercial purposes would be slightly unethical, since it would be feasible to resell histories over and over again, which, according to Kantianism, would be using the people as a means to an end. Of course, where a crime is involved, exceptions can be made. In order for this technology to be used in other countries, it would be necessary for the terms to be applicable in their country, and it would have to be possible to make sure the governments of these countries would obey the terms, without circumventing the terms of use to needlessly punis their own people.

1. **of opt-in feature,** some say opt-in, and some say opt-out. No agreement here one way or another. *[ananth]*

Anonymous 2732
04/09/2014 07:34 PM

Professional, ethical, legal, and social issues and responsibilities.

The most significant ethical issue that we must consider is personal privacy. The concept of an opt-in policy will ensure that the privacy rights of individuals wil be respected. This is ethical from a Kantianism view point, and also fulfills the principles of respecting the rights of others and treating others justly. Secondly, the relationship our company will have with law enforcement ensures that we are disclosing information to those who should know, and allows the social contr to be enforced.

Anonymous 2719
04/10/2014 10:22 AM

It is our responsibility to be impartial by putting the good of the general public in front of the gain of our company. By not selling the the habits of specific people or people's location we can effectively achieve this. It is important that the system does not store information such as where an individual lives or where an individual frequently shops or visits. Although it would be very profitable for this action to be taken, it would not benefit the general public and even if the information was not sold, the risk of this information being hacked or leaked is unnecessary and could be detrimental to many people's lives. The system must be very secure and with a log in user name and password that requires the user to log in every time. It is our responsibility for the system to time out after 20 minutes to ensure that the person on that account is the actual person using the account, this will help us to treat others justly by protecting their privacy. As a global rule that would increase net utility our company upholds that "Users should only ever access their own accounts on any platform". By creating a password and the time out feature we are upholding this rule and it is ethically correct by act utilitarianism.

Anonymous 2732
04/10/2014 10:54 AM

Yes, security is very ethical by act utilitarianism. But it also fulfills the principle in the code of ethics that states that we must take responsibility for our work. Of course with respect to privacy, we must find a balance between the individual's expectations of privacy and the amount of information we provide.

Anonymous 2717
04/10/2014 11:42 AM

We also have to strongly consider having a specific, very secure database for Law Enforcement. The reason being, we have an opt-in standard, but there should be an exception when it comes to criminal activity. To counter this being abused, I feel that each time it is accessed, it must be by court order, and only by a high ranking LEO, like the chief of police. I think this would still protect the public's right to privacy, and it would also keep them safe by somewhat controlling criminal behavior.

Anonymous 2730
04/10/2014 04:59 PM

Even with an opt in strategy we would need to make sure that other companies that use our software have an opt in policy that is easy to understand and doesn't have extra parts that deceive the user. As long as the user knows exactly what is being done with their information and approve of it we are able to stay ethical under Kantianism.

Anonymous 2717
04/10/2014 07:38 PM

It seems we agree entirely on the opt in approach, which would more or less fulfill the requirements for ethical behavior under social contract theory, as long as everyone agrees to not misuse our software. We would also have to consider the case where a user misuses our technology, by stalking or other means, in which case we should be able to track who was looking at what location.

Anonymous 2732
04/10/2014 10:55 AM

Local and global impacts on individuals, organizations, and society

The overall impacts of this technology on society and individuals would be that individuals would have less privacy and society would have greater access to information about certain individuals. With more knowledge about what occurs in public places, law enforcement would have an easier time solving crimes tha are recorded by this technology. Organizations who use this technology would know much more about certain individuals to create targeted advertisements. Individuals would have to be much more conscience about where they go or how they act in public places.

Anonymous 2717
04/10/2014 12:00 PM

Globally, this is a somewhat different challenge, because even if we set rigid standards for how our technology is used, that doesn't mean that governments will respect our terms of use. For example, what would be stopping a corrupt government from hacking into our system, or replicating our technology and abusing it? These are things we don't necessarily need to address in the US, but it does pose a bit of an issue. On our end, we can protect ourselves and our databases, but we can only do so much to protect the rights of others around the globe, an issue I feel we definitely need to tackle somehow.

1. **These are things we don't...**
Seems to be making an arguable assumption here at US governments are not-corrupt, and that if it is a corrupt government it has to be from outside. *[ananth]*

Anonymous 2732
04/10/2014 02:26 PM

The impact of this technology in foreign countries is definitely something to consider. Since we have to adhere to international laws and the laws of each government, it's only fair that governments using our service must adhere to our terms of service. Of course, we must provide the best security to ensure we are not hacked.

Anonymous 2719
04/10/2014 02:26 PM

We will not be selling information about the people using our software to organizations because we do not want to treat our customers as a means to an end, but there is no way to guarantee that people will not be data mining themselves. Unfortunately our system will change the way organizations advertise to certain individuals living in specific places, this is one of the reasons we have an opt-in feature so that people know the risk of being identified in our system and are still being treated as rational beings.

Anonymous 2730
04/10/2014 05:27 PM

The thing is even if we are not selling customers information companies using our software may even if we have a terms and conditions that they use. There is no easy way to tell if another company is selling information.

Anonymous 2717
04/10/2014 07:29 PM

I suppose we would only have to be responsible for our own company's actions, and do whatever we can to make sure our software is error proof. If other companies copy our technology, and misuse it, we can only control what we do, and it would fall on them for their misuse.

Anonymous 2719
04/10/2014 08:11 PM

I completely agree that other people will be selling information gathered by our software, I think the ethical thing for us to do is to make that information not readily available and rather make that information as difficult to attain as possible while still making our system useful at the same time.

Anonymous 2730
04/10/2014 08:25 PM

As i said in my initial post a way to make it so the software is useful but not giving all information like for businesses it would show how many people are at a shop at given times which tells the company when they may need more employees or times when they can have less saving them money without giving any specific information on an individual.

Anonymous 2732
04/10/2014 12:10 PM

Further knowledge and research needed

Since we are using the latest facial recognition technology to identify people, we must know how accurate it is and also what aspects of the environment may affect its accuracy. We must know how much lighting effects its accuracy, then find a way to make the proper adjustments in low light environments. Additiona we must know how the current privacy laws apply to this system. To do so, we can look into court rulings on similar cases that may apply to our system.

Anonymous 2719
04/10/2014 03:16 PM

More research is needed to figure out who will let our system use their cameras. It is also important to firgure out what video feeds we will be able to stream live and what videos will only be available based on recordings. We decided that only police offers would be able to view recorded data so this will play a large role on our commercial use of our product and on our funding.

Anonymous 2730
04/10/2014 04:39 PM

Looking into http://www.extremetech.com/extreme/178777-facebooks-facial-recognition-software-is-now-as-accurate-as-the-human-brain-but-what-now shows that the facial recognition software is 97.25% accurate. This helps in dealing with the concerns about false positives with the system, although there is still a very slight amount of error.

Anonymous 2717
04/10/2014 07:33 PM

Another point to consider is people that look very similar, such as identical twins. Obviously, this is a pretty extreme case, but the point still stands that it would be nearly impossible to distinguish one from the other, in the case of criminal activity. Over time, we can assume facial recognition software would improve, or we can work on it ourselves, since we would be fully responsible for any errors that occur.

Anonymous 2732
04/10/2014 02:40 PM

Biases and assumptions.

As stakeholders in the company that provides this service, it is within our best interest to earn as much revenue as possible. In order to do so, we are inclined market large amounts of information to our clients. To make sure that we do not infringe upon the rights of individuals, it is imperative that we find a balance between our corporate responsibilities with our moral responsibilities.

Anonymous 2719
04/10/2014 03:35 PM

Everyone we sell information must be from a legitimate company and not just an individual after someones personal information. If we use this as a universal rule we can conclude that there will be an increase in net utility. By rule utilitarianism and by Kantianism we will keep this rule to be ethical and at the same time still gain a profit. We will keep this rule to treat our clients as rational beings and not a means to an end.

Anonymous 2730
04/10/2014 04:49 PM

[no notes on this page]

The only way we can stay ethical is by making the software difficult to change otherwise a company using it would be able to change the way it works and abuse its functionality. Even if we made the company abide by some terms of the service it doesn't stop them from trying to go around it. Another issue is that even if we try to keep from infringing on peoples privacy a company using our service can still sell the data they get to other companies.

Anonymous 2719
04/10/2014 08:08 PM

One way to avoid having to sell people's information would be to charge a subscription fee for our services, then we could keep peoples humanity by not selling their personal information. This may be more ethical than data mining.

Anonymous 2732
04/10/2014 08:15 PM

One assumption that we could make is that our clients will adhere to the contractual agreement and not use the information in an unethical way. Of course, this may amount to signing an agreement and looking the other way. So we should take a more proactive stance to ensure our clients are doing the right thing.

Anonymous 2717
04/10/2014 08:19 PM

That brings up a good point, of how we would stop other companies from using our product for commercial purposes. Perhaps we could come up with a commercial version, where we would charge another company for the rights to use the information they gather. Since the people opted in, it would not be using them as a means to an end per se, and it would be a reasonable way to defer responsibility to the other company, assuming we create a sturdy enough disclaimer/terms of use.

Anonymous 2730
04/10/2014 08:30 PM

I really like the idea of making it so the companies that use the software have to pay for information they gather. This is a great way to keep our product used for only certain uses like for targeted advertising and such.

Anonymous 2732
04/15/2014 07:56 PM

Policy Statement

The main topics I think we must cover in our policy statement include security of our data, access to our data, and privacy issues. Of course, we should also address how it may impact various stakeholders including: the public, our clients, and law enforcement. One idea to consider concerning privacy and access the possible leakage of information. We should state our liability in the event our database is hacked, or if one of our clients leaks certain information about individuals. The licensing agreements that we outline for our clients and for individuals should be created with the utmost transparency. Also, we should define what information may be considered public and private and who can access private data. I look forward to hearing your thoughts on these topics.

Anonymous 2717
04/17/2014 12:15 PM

Security - Obviously we need the highest security possible on our servers, to both protect the clients and the public, and to protect ourselves from the repercussions of exposing a massive amount of information, albeit unintentionally.
Access - I believe we can agree that an opt-in approach is best, since that way, the public can choose to be a part of our system, rather than having to discover it and opt out. A second server should be only accessed by law enforcement, or just another segment of our main server, but as far as security goes, a second server would probably be a better option. Regulations should be in place to avoid unauthorized access to our secondary server, so the police can't just access it whenever they choose. Obviously, we discussed a commercial option, where we could charge companies for access, likely based on a certain charge per person/profile accessed.
Privacy - This is the hardest part in my opinion, as we have to respect the rights of individuals while also more or less tracking their movements and habits. For example, our secondary server would just identify people without consent, which is why it needs to be secure, while the primary server would only have a limited amount of information regarding people and their habits.

Overall, as long as our security on our servers is at a maximum, we should be able to cover ourselves as far as liability concerns go, and we must also make sure that we can only allow access to our law enforcement server to a high ranking officer, and input the warrant data so we can protect the rights of those that are contained within the server.

Anonymous 2719
04/17/2014 12:31 PM

As for privacy, I would like to ask the question: Will we be selling information about people for advertisements and if so how do we want to do it? I read the section above and I found that we are all over the board on this idea.

Anonymous 2732
04/17/2014 01:27 PM

[no notes on this page]

My thought on personal information privacy, is that we have two levels of information about people. The first level should be considered public and should not intrude on anyone's privacy rights, meaning that we can show how many people visit certain locations, but no private information about those individuals. The second level of information must have an opt in policy for people that are willing to share information about themselves such as their identity and the locations that they visit and certain times. The first level can be more easily accessed and the second level can be sold to clients.

Anonymous 2717
04/17/2014 01:35 PM

I like the idea of having two levels, since some things are going to be public anyway, such as cameras in public places. These would be available for free, for people that just want to monitor traffic in a certain area or something along those lines. Selling information to clients is going to be tricky, as what kind of information should be considered marketable? Interests, places visited, or what else?

Anonymous 2730
04/17/2014 06:15 PM

We also need to think about how to deal with law enforcement. Are we only allowing them information on a person after they have gotten a search warrant. And what kind of work will be done to get access to private security cameras. For selling information we can use people who have opted in and it will allow companies to create specific ads for these people.

Anonymous 2719
04/17/2014 06:32 PM

Since we will be selling this information I don't think search warrants will be required. The police will have to pay for the level 2 footage just like everyone else if they plan to use it. We will let the courts decide if they allow people to use our footage in court.

Anonymous 2719
04/17/2014 06:45 PM

So, everyone will be in level 1 because it is public property and for level 2 we will have an opt in approach where anyone can submit information about themselves, but to allow access to the video feed you also have to pay a subscription fee. We will not ever show video of private property. I think discounts should be given to those whom submit information about themselves and also want level 2 access.

Anonymous 2717
04/17/2014 07:01 PM

I still think there should be a server just for law enforcement, but we can work around having them pay for special access. I just think it would help out society more by having all footage on record in the case of a crime being committed, but that could be seen as using the population as a means. So it sounds like making police use level 2 access would be suitable.

Anonymous 2730
04/17/2014 07:05 PM

So we would allow more than just businesses to use level 2 service. And i think that giving discounts would be good, but for a company what would the stipulation be for giving them discounts?

Anonymous 2719
04/17/2014 07:08 PM

How do we feel about letting only the law enforcement see our "level 3" access which would be recorded video? We could then limit level 1 and level 2 to real time live video, this would increase the privacy of our users and also help the police solve crimes. If we do this we will also need to have far more secure systems for storing the video.

Anonymous 2732
04/17/2014 07:20 PM

I agree that helping law enforcement is very beneficial for the public and for our company. We can justify this using Social Contract Theory and the code of ethics. We could also form an agreement with various law enforcement agencies and treat them as a client.

Anonymous 2730
04/17/2014 07:26 PM

That sounds good, but the thing is how long will we keep footage stored because that would take up a lot of space quickly depending on how many cameras we are using. Also if the person they are looking for has not opted in we would not have much specific information on that individual.

Anonymous 2717
04/17/2014 07:30 PM

[no notes on this page]

I like the idea of level 3 access, it's a nice compromise to our situation. I figure we can keep footage for 6 months, unless it catches a crime, but I assume the police will already know where a crime occurred, and want to search those cameras nearby. However, if we keep a database, we can give them quick access, and we could also use this to our advantage and let the law enforcement use it for a fee or a contract, or something along those lines.

Anonymous 2730
04/17/2014 07:40 PM

I think that we will have to use some kind of contract to make sure that footage is used legally and without taking advantage of it.

Anonymous 2719
04/17/2014 08:00 PM

Lets keep the footage for 1 year, but we will give the law enforcement agencies a copy of the footage if they need it.

[no notes on this page]

Team Project Discussion - Team 03

Toggle Anonymity

Select Discussion: Team 03

Please see attached prompt and rubric.

Enter new discussion post here...

Post

Anonymous 2708
04/03/2014 12:25 AM

In order for our company to successfully create the webcam history technologies there are many topics that our polices must cover including privacy, security, and where and when our technologies will be used. This technology's main goal is to provide a searchable history from data gathered by security cameras an processed with facial recognition software.
To achieve this goal the system at its most basic level will need to collect images of people through cameras in a variety of places in public. These images ne to be high resolution and as front facing portrait as possible. In order to create this database with useful information the program will need both first and last names of the people being identified and that name tied to an initial photo to use for comparison.
This system would best be served by an Opt-In system. This falls in line with Principle 1, clause 1.06 which states that Software Engineers, "be fair and avoid deception… concerning software". Having an Opt-In system also protects people who the public feels requires privacy of location such as high power politicia for example. This will also be a benefit because those who Opt-In may be more willing to supply their name and multiple pictures which will make recognition the individual much more accurate. One major downfall for the company with an Opt-In system is that we have less people participating in the software, with more people in the database the facial recognition software can be trained to better recognize and differentiate people. This is supported by Kantianism whic says people must be treated as rational beings, by giving them the choice, they are able to make the final decision for themselves and are not being used to better the software.
This system would be implemented in only the United States (at least initially). Making a facial recognition and history system in other countries can cause conflict with other cultural norms as well as local policies and laws. For example in countries where the government has rights to internet history and use it to prevent demonstrations and riots against them, they would be allowed full access to the information in the system. This would infringe on our western values o right to free speech, demonstration and privacy that we generally believe should extend to all people. This may also conflict with our policies about who is required to have a court order to access our data.
The ethic clause 1.05 support readily supplying information, "to address matters of grave public concern" but this is contradicted by 2.03 which states only, "u the property of a client or employer only in ways properly authorized, and with the client's or employer's knowledge or consent". In this case I would lean towar requiring a court order in all cases because readily giving out information may give out that which is beyond the scope of necessity for government or police forces to do their job which may cause an uproar about privacy. Thus a court order will assure that necessary parties only receive information they need base upon a third party (judge) review. A court order also assures the company and their clients that unnecessary information is not made public.

Anonymous 2713
04/04/2014 04:20 PM

A company should support any software that it creates as long as that piece of software is legal in the area it is used in. If it is software that records every sing person that walks by measures their height approximates their weight takes down characteristics facial recognition and posts it all on the internet, this is an actual piece of software that could do very well in the right market, would large companies and public companies use it? Probably not because the social backlash would be a huge factor in their decision. Do I think it is a good idea to create something so "privacy infringing"? No I do not, but only for the reason I not believe it would be a profitable venture, is it super cool and advanced? Yes. If the person is walking in a public location there is no protection from their likeness being used anywhere as long as you own the picture or video, we can see this from paparazzi photos and videos. So I doubt there is any protection about facial recognition while you are in a public place, if the camera is set up in a non public place then I believe you have to have a disclaimer. Under Socia Contract Theory however this would be seen as ethical because you are not breaking any contracts or laws, while most people assume they have a right to privacy while they are in another location that they have not rented, own, leased or otherwise controlled they are not on their own property and therefore canno assume any protection against someone viewing them. Video cameras are complicated because there can be an issue whether they are recording and stori the video or if they are just using real time data, and how much they are recording. If they are using real time data and using a relatively small cache I do not believe they can be classified as recording an individual which would be a loophole around many small laws. As stated previously there is no laws about bein recorded when you are on public property, there is also no laws if I am on my property and watching outside from my property at your house, I can have a camera aimed in your living room window and as long as I am on my property I can record what happens within the line of my sight from my property. Places t should not be viewable by this software would be private interior property that the owner has not allowed to be viewable by the cameras, rooms cameras are specifically not allowed in such as dressing rooms and bathrooms, while I believe the company should have an opt out option for people they legally do not ha to do this, and ethically following social contract theory. The company should have some sort of limitation concerning underage persons, such as if the person found to be underage it would not be recorded or posted online, another consideration would be the company should not provide any information that is not publicly accessible online should not be posted online.

Anonymous 2705
04/04/2014 07:17 PM

1. **For example in countries...**
Recognizes that not all societies have Western values, but oversimplifies and is culture-centric with an implicit assumption that western values are somehow more valid. *[hauser]*

2. **it super cool and advanced?...**
colloquial. *[ananth]*

3. **no protection from their...**
awkward phrasing. *[ananth]*

4. **many small laws.**
?? *[hauser]*

5. **As stated previously there...**
Assuming oneself to be an expert on the legal aspects across the country and around the world. *[hauser]*

First off, I would not be involved in this company. There are too many ways this could go wrong, and personally I take issue with the proposed project. My own reasons aside, let's assume this is a company that I care about and that I want this idea to move forward, of course I am going to support it.

As it was described, I think the most arguably ethical and legal way to propose this company's project would to be as a service based on currently existing infrastructure, instead of a new technology. Unfortunately people in general have a misconception about privacy, and this is part of where the company would have to be careful about which 'providers' (of cameras) they choose.

By Social Contract Theory, the people being viewed need to understand that while they are on public property they are consenting to being observed. Those people have have a right to 'opt-out' of being observed, and that is called going home, closing the blinds, and hiding in their basement which is all on private property. If cameras are placed on private property and following people around to build a profile of them, that could be considered stalking. By utilize the cameras in place (on private property) already, the company would be utilizing an infrastructure already in-place and offering a public and government service

I definitely think that all data flowing across the company's network, website, etc should be encrypted and the data on their servers. I assume the access to this service would be to citizens of the United States (if it's a USA provided service), as the citizens should be following the laws of the land and those in other countries may not be held to the same contract.

It would be the responsibility of the company to ensure that the provided cameras followed any necessary set of requirements.

Anonymous 2729 1
04/04/2014 07:34 PM

It is my opinion that it would be essentially impossible to develop this kind of technology and utilize it ethically. According to social contract theory it migl be possible to formulate an argument that nothing in the mission plan is illegal therefore it can be considered ethical. I don't see this as an accurate way to frame the issue however, it would be completely impossible to obtain consent for everyone involved who is seen by these cameras and whose location will be reported. While technically it is true that people implicitly consent to being recorded in public I think you would be hard pressed to find any way in which our company would be considered NOT using people as a means to an end. There is a clear and obvious negative impact on every single person that is identifie and geo located by our software which could number in the thousands or hundreds of thousands and whose negative utility from the loss of their privacy far outweighs whatever minor gain in utility government agencies and private enterprise gain by being able to track people's behavior patterns.The potential for abuse of a system like this in a restrictive society is beyond astronomical. Attending a political protest would be essentially impossible as you would be observed going to the protest by cameras and could be identified and arrested (or executed) days later. Corporations could use the technology for union busting practices, or to prevent their employees from seeking better employment by having the system alert them whenever one of their employees was spott by a camera near their competitors operations. This technology would undoubtably be used by the elite and wealthy of society to oppress the less advantage would be beyond unethical for us to develop and sell this technology, and now that we have identified that such technology is possible it would be unethical for to allow anyone else to develop it as well, this leaves us with only one real ethical option.

In order to handle this issue ethically we will develop this technology, we will patent this technology, and we will defend our patents aggressively. We will never however, sell this technology. We will become the world's first ethical patent trolls. We will use the flawed American patent to permanently stall technological development in this area. To use an admittedly weak metaphor we just stumbled onto the free speech equivalent of the recipe for weaponized smallpox. To s it would be horrendous, to allow others to sell it would be just as bad. Thankfully the flawed American patent system will allow us to stop this technology from existing for as long as we can keep our patents valid. The second another company or the government presents or proposes a system similar to the one we have developed we will sue them with absolutely excessive force. We will use the profits from these lawsuits to finance further developments of the technology and further patent applications which will allow us to extend our ironfisted grip on this technology and ensure that it would never fall into less ethically minded hands.

We have a rare opportunity here to prevent a horrific human rights violation from being made manifest. Don't let this opportunity waste away. We can be the greatest of heroes, or darkest of villains, your choice.

Anonymous 2703
04/04/2014 08:16 PM

First off, this is not a technology that I would have any rational or ethical desire to participate in. I believe the best course of action may be to patent this information to keep it out of the hands of anyone who has the (inherently creepy/malicious) intent to track people's everyday movements. There is no reason I support that this technology should ever be used, and I would say this is a stance that has significant grounding in Kantianism.

But I think looking at legal implication is an important step to examine here. Let's assume this is for deployment in the US, for the sake of one particular legal system. Case law in the US has upheld a fairly high standard of privacy in private residences, in cases such as Mapp v Ohio and Lawrence v Texas. Which ruled on unreasonable seizure during warranted searches and consentual sex in private locations. The courts have however never held a standard of privacy f public places. Cases such as children, or entertainment (often reality tv) are some exceptions that require releases. This would most apply if the potential customer was for profit, and wanted to make say a TV show that follows people that have no idea they're on a show. Like the Truman Show, but in a totally public environment with little to no support crew. Law enforcement use could also be in a very sticky situation about the evidence gathered from places that ha an "assumed level of privacy". Additionally, if we use the example of individuals to use this technology, this would facilitate stalking and other privacy interrupti activities. So, from the view point of a social contract theory, it seems there may be way too many illegal uses of this technology. Even in the case of uses that are legal viewing of people in public places, it is still a violation of their natural right to privacy. While potential illegal uses seems to be a weak reason to rejec technology, any legitimate use of it could be solved in a way that is effective enough and presents significantly fewer potential legal and ethical objections.

From a kantian viewpoint, facilitating the tracking of people nearly anywhere outside their own homes is substantially invading their privacy and absolutely not treating them as rational beings. This technology will inevitably lead accusations and excessive litigation that would be unnecessary, not allowing the people t act rationally and in their lifestyle without harassment and interference. By invading the absolute limits of private space for any commercial use (well possibly legal) is treating them as a means to an end.

I believe that the brazen violations of both social contract theory and kantianism indicate that this is not an ethical technology to develop. So, in terms of technologies I think should be developed would be anything that is both patent-able, and essential to the deployment of this "tracking" technology. Once that technology is locked down, it would be the task of being heroic patent trolls to prevent this technology from being deployed to any private, commercial, or law enforcement use.

1. **Anonymous 2729 04/04/2014...**
Apart from the fact that might own opinions lie close to this poster's, this is also the first analysis I've seen that seriously considers the perspective of the "public" non-users and considers in an at-all realistic way the consequences for those people. Let's see what others say to this. *[hauser]*

2. **But I think looking at...**
The legal perspective. Interesting that they missed United States vs. Jones, the Supreme Court GPS tracking case from 2 years ago. *[hauser]*

Anonymous 2708
04/08/2014 10:29 PM

FURTHER KNOWLEDGE AND RESEARCH NEEDED THREAD:
Nick was able to site Mapp v. Ohio and Lawrence v Texas for private surveillance rulings but we still need cases, laws or something (if there is anything) on surveillance in public space. For example those who have store front surveillance does that count as strictly private although it may capture those walking by t store?
Bryce also mentioned the paparazzi, which lead me to find: Senate Bill No. 606: An act to amend Section 11414 of the Penal Code, relating to harassment which was signed by the California governor on September 24, 2013:
"Any person who intentionally harasses the child or ward of any other person because of that person's employment shall be punished by imprisonment in a county jail not exceeding one year, or by a fine not exceeding ten thousand dollars ($10,000), or by both that fine and imprisonment." With the details being, ""Harasses" means knowing and willful conduct directed at a specific child or ward that seriously alarms, annoys, torments, or terrorizes the child or ward, and that serves no legitimate purpose, including, but not limited to, that conduct occurring during the course of any actual or attempted recording of the child's or ward's image or voice, or both, without the express consent of the parent or legal guardian of the child or ward, by following the child's or ward's activities or b lying in wait. The conduct must be such as would cause a reasonable child to suffer substantial emotional distress, and actually cause the victim to suffer substantial emotional distress."

This description is not directly related to video surveillance but is a good indication of the problem with taking video of children let alone running facial recognition. So more research into the public space and rules about children will be very important.

Anonymous 2729
04/10/2014 07:57 PM

http://management.fortune.cnn.com/2013/04/26/video-surveillance-boston-bombings/

According to the article there are an estimated 30 million security cameras in the United States. That's one camera for every 10 people (roughly). Spaced somewhat intelligently one could easily see how you could keep the majority of American citizens on camera the majority of the time. Additionally the article mentions that in the wake of the Boston bombing even more cameras will likely be deployed. Before anyone tries to claim that this doesn't apply because not all of these cameras are public facing I would like to point out that our prompt specifically states that our company would attempt to negotiate with owners of other cameras to obtain access. I think that this is important to consider because it gives a good idea of how incredibly powerful this kind of technology could be. There would be people who would spend their entire lives under the gaze of our cameras, and whom our algorithm would know completely.

Anonymous 2713
04/10/2014 10:45 PM

http://www.cbc.ca/news/canada/british-columbia/stanley-cup-riot-prompts-call-for-more-cctv-cameras-1.1092239

Penny Ballem states "The availability of closed-circuit televisions was invaluable to the response efforts during the riot in providing real-time information to all responders," in a report prepared for the city. There are many cameras installed already in Vancouver and some groups are asking for more to be installed. This is because many people have been convicted of participating in riots after the Stanley Cup let down in 2011. Other privacy advocates reiterate that cameras do not significantly prevent crime and do more harm to privacy than good for security.

Anonymous 2708
04/10/2014 11:16 PM

I found the last line of Alex's post intreguing because this could very well happen and as we know we tend to be creatures of habit. A person's daily routine could be determined soley from the use of surveillance cameras. This could be used for good in terms of making life easier for people, for example if they go to a specific coffee shop every morning the coffee shop could buy this information to learn more about their customers and their habits, combined with that company's data could provide better and faster service. But as always one of the downsides could be stalking. This would go beyond what we currently think as extremes in online stalking through social media posts because it would be specific date-time stamped events. How then do we handle prevention of online stalking? Or stop online stalking once someone has access to the data? Security would have to be extreme, which in our rapidly changing technology would be impossible to keep under 100% lock down, especially over a long period of time.

Anonymous 2703
04/10/2014 11:38 PM

While it is interesting that there are a few cases where this technology would be very useful in law enforcement, but in the whole literature concludes that cameras do little to deter crime. Maybe it's just an issue of crime prevention vs catching after the fact, which would serve to still have the harms of the crime and put another person in an overcrowded jail that is likely to only exacerbate mental health issues. But this isnt a discussion of prison conditions. Also, additional information is needed about the requirements to use public footage for profit. There must be a reason documentaries need releases from people. This is important given potential reality show. As far as the stalking issue, it seems to only be a more extreme version facebook stalking ethically. If we go with the opt-in approach, I think it can be treated the same way.

Anonymous 2729
04/10/2014 11:54 PM

I wonder if this technology could also support filters for searching for specific demographics and geographical locations as opposed to specific people. I could see some very problematic situations with people searching for "single women who walk home at night and go past a dark alley" or something similarly sinister.

Anonymous 2705

[no notes on this page]

04/10/2014 11:54 PM

Cameras NOW do little to prevent crime, but if people knew that their being no camera was directly related to a profile built up about them... I feel it would be a very different story.

The only possible way I can see the report by privacy advocates stating, "that cameras do not significantly prevent crime and do more harm to privacy than good for security," is if the privacy of one person can be considered more valuable than the safety of another. Looking into this, there is somewhat a domain locality to be considered. Is a person's privacy (body space, free will) worth more than their inalienable right to life?

Anonymous 2729
04/10/2014 02:03 PM

LOCAL AND GLOBAL IMPACTS ON INDIVIDUALS, ORGANIZATIONS, AND SOCIETY THREAD:

It is my sincere belief that this technology will have large scale impacts on individuals who have any reason whatsoever to keep their personal movements confidential and private. As I mentioned in my initial post I think this technology would be a godsend for anti-union businesses as it would allow careful monitoring of the comings and goings of its employees. Additionally it would make it very difficult to attend protests without identifying yourself with that politica cause explicitly. It would also make it easy for businesses to prevent their employees from talking to other businesses they might want to seek employment fro Overall it would have negative impacts for freedom of expression, freedom of work and freedom from scrutiny. Sure all of the data is already there for use but a far cry from having the data available to actually indexing and cross referencing and building a database for anyone who can and will pay to get the access. Over all I would rate the local and global impact on individuals as Dystopic. For organizations it would be either beneficial if you have a lot of capital or strong social standing or catastrophic if you have neither capital nor social standing. Counter culture movements would be incredibly dangerous to be involved in and would thus wither and die. Society would lose a huge amount of alternative expression, which historically has been very beneficial for society as a whole. We would become homogenized and horrifically boring. It would LITERALLY be 1984.

Anonymous 2708
04/10/2014 04:28 PM

I agree with Alex's views on the impact this system would have. Expounding on his point about public protests (especially of the political nature) in the global community where the government has more power over individuals. There is already the potential for extreme punishment if it is found online that you were at a protest (via photos, posts etc.) to have everyone captured on video there would be a smaller margin of error in determining who was there and participated in the protests. In civil liberties that many in the united states disagree with would be more enforceable, such as countries where women must be escorted by a male (usually relative) and/or have themselves covered.
On a more positive note, beauty parlors, makeup companies, wig makers and shops, and plastic surgeons would have business boom with people looking to find ways to make themselves less recognizable in the video footage.

Anonymous 2713
04/10/2014 11:20 PM

The clients that would be buying this are mostly companies, and like it or not companies are only thinking of the good of the company, and they will use anything they can to increase revenue for the company. If employees are protesting something the company is interested in this can be used against the employees and this is a very bad thing. People would not feel as safe to express themselves as much and society would decline. We wouldn't want companies to view our social networks like some were requiring previously why would we want them to know where we are at and when we are there and what we are doing?

Anonymous 2729
04/10/2014 11:38 PM

It's interesting you bring up companies abusing social media because there was just recently a case in which the courts upheld that companies do not have the right to ask for your social networking accounts.I wonder if that case could be seen as setting a precedent for making this sort of thing illegal as well.

Anonymous 2729
04/10/2014 11:38 PM

It's interesting you bring up companies abusing social media because there was just recently a case in which the courts upheld that companies do not have the right to ask for your social networking accounts.I wonder if that case could be seen as setting a precedent for making this sort of thing illegal as well.

Anonymous 2705
04/10/2014 11:43 PM

This certainly poses an information availability risk, if that makes sense.

I don't see how people wouldn't feel safe expressing themselves. Do you think society might act differently if they always knew they were under watch? - less/more murder, vandalism, tom foolery, prosecution (race, gender, etc), chicanery?

Anonymous 2703
04/10/2014 11:47 PM

I agree wholeheartedly about the dystopian potential of this technology. The effects it could have on politics and economics is nothing short of

[no notes on this page]

terrifying. Political demonstration has long been a pillar of political expression, and the fear of being recognized would stunt these both by be a deterrent to participate or by incarceration. The effect of making employees terrified of their bosses reminds us of The Jungle and the Communist Manifesto. There isnt much else to say beyond the fact that this technology would easily facilitate what is widely considered a nightmare of a future.

Anonymous 2708
04/10/2014 11:49 PM

Thinking about how society might be different under this kind of surveillance I think about Prohibition and Underground railroads. Any major political movements, anything against the law etc. would have to go deep underground (almost literally) in order to avoid the cameras. So I don't necessarily think crime would drop a ridiculous amount it would just move to other unmonitored spaces. For example vandalism would become much more contained once someone figured out where there is a wall or something that wasn't being watched. I am sure soon after a software like this emerges there will be a counter movement to either shut it down or to find its uncovered area which is another whole set of information that would take the market by storm.

Anonymous 2729
04/10/2014 11:51 PM

Literally 1984. Except even easier for the bureaucratic machinery to maintain control because its all automated.

Anonymous 2705
04/10/2014 11:57 PM

Ok and is that a problem - if everyone is being treated the same by bureaucratic machinery then by Act Utilitarianism, are we not able to glean the most beneficial path?

Anonymous 2705
04/10/2014 02:19 PM

BIASES AND ASSUMPTIONS:

Bryce and I seemed to have a similar opinion/understand that privacy on public property is not a written right that has been defended in a way that directly conflicts with the abstract of this service.

I suppose it might be correct in saying that I am bias about the ability and/or danger to implement this project because I assume there is a lack of privacy as it and people really don't care that much (aka, why not - no problem). If anybody uses Google anything (mail, search engine, games, operating system, browser especially if you log in), I automatically assume that they understand they have a profile built up defining who they are, where they go, what the search, who the talk to. To those that say there is an issue where the information could be used against them, what's from any company like Google from using the information they have accumulated?

Let me ask you, for transparency wouldn't it be better if everybody had access to that information, or do you only care if someone is trying to sell you stuff (like Google and every other add company ever).

If anyone is concerned about their information being released, an easy fix is to have the databases only release information about people that have opted in t this service. Just because a profile is being built, doesn't mean it will be released.

Anonymous 2729
04/10/2014 07:49 PM

As my posts have probably made clear here I have a pretty extreme bias against this sort of technology. Obviously I can not be counted on to treat these issues objectively as I find the very idea horrific. To answer your question I don't agree with your presumption that everyone would have access to this information, I assume that a hypothetical company would want to charge money for their service which means that we are paywalling who gets to see our data from the very beginning. This creates an intrinsic power disparity in who gets to use our service. The haves get to use this information, and the have nots (who cant afford to buy their way past our paywall) do not.

I also MASSIVELY disagree with your presumption of "Just because a profile is being built, doesn't mean it will be released." First of all, you can't assume that at no point the service will ever be compromised and have it's database leaked. Second, you have to assume that the government is going to supeona for access to this sort of data either on a case by case level or constantly. Third if the company is ever sold there is no guarantee that the new owners would have the same ethical considerations that we do with regards to people's privacy. There is no way in which collecting data but not disclosing it does not endanger people's privacy regardless.

Anonymous 2713
04/10/2014 09:32 PM

The issue with this program is the central principal, mass intelligent surveillance, the majority of people will not want this, If I had a choice to decide if I would allow it or not I would not allow this, I assume many other people would feel the same, that being said I do not think it is even a remotely good idea to develop this, maybe for a country that doesn't have the privacy rights that we do, but for the United States this is an inherently bad product. I do not think that it is correct, to implement however I do not find that it is illegal. Should it be? probably. Is it? I do not think so. More privacy is better all hail freedom.

Anonymous 2708
04/10/2014 10:49 PM

[no notes on this page]

When I first looked at the idea of a webcam history I envisioned a public website with a Google like search engine. With that being my first impression (or rather thought) it has been hard to move into thinking about something more locked down with limited access which is what a tool like this would have to be. The second thought for me is internet and privacy, I have basically come to terms with the fact that anything that is put online it is no longer secure nor private. With this in mind I cannot imagine having a tracking website such as this online even if there was a way to properly secure it.
Thinking about one of the topics in class where much of the government is questioning mass collection of phone numbers and information through the NSA and the Patriot Act then there is no way a company could survive the public backlash of this type of mass surveillance system.

Anonymous 2705
04/10/2014 11:14 PM

I suppose I had figured the information would be more available than not, like a "free" service (similar to facebook or google search - free as in free stuff, not freedom). That is a very good point to consider.

In the world of technology, something like this would have to be at the leading edge of security/encryption/etc. This is just reiterated this last week with SSL Heartblead information being released about openssl. I hadn't thought about the prospect of selling the company. Is there a way we could formulate our EULA company such that after being sold, users would be protected?

Anonymous 2713
04/10/2014 11:36 PM

There are so many unknowns with this project, what the contract between the software maker and the client would be and to what extent the information found could be used for. If we are assuming the worst of a situation which I believe we can, this would be a terrible software for one entity to own, yes it would technologically advanced, but so would a super virus, just because you can create it doesn't mean you should.

Anonymous 2713
04/10/2014 11:36 PM

There are so many unknowns with this project, what the contract between the software maker and the client would be and to what extent the information found could be used for. If we are assuming the worst of a situation which I believe we can, this would be a terrible software for one entity to own, yes it would technologically advanced, but so would a super virus, just because you can create it doesn't mean you should.

Anonymous 2729
04/10/2014 11:44 PM

@Andrew
Well whatever company bought the surveillance system would still have to abide by the original terms of use, that being said our assumption is that we would be collecting data and building profiles without people explicitly agreeing or even being aware of the system's existence. This would probably be legal because of the laws in place that we have no expectation of privacy in public, so it seems unlikely that a new and potentially sinister company would feel the need to uphold implied contracts they did not actually sign and had no baring on.

Anonymous 2703
04/10/2014 08:59 PM

Professional, ethical, legal, and social issues and responsibilities:

First let's look at the ethical differences between our proposed policies. The different ideas largely come down to "opting in" or "opting out", or choose to not deploy the software at all. The strongest ethical framework opposition to this technology would of course be Kantianism, primary the whole treating people like "rational beings" and "a means into themselves". The opting-in approach would solve this potential issue, as would not deploying. Also, opting in would mitiga the social contract theory issue, and would make it more ethical by the ACM code of ethics by letting people know what they ought to. So, it would seem many the on face privacy issues could be reduced by using the opting-in or refusal to deploy policy options. Additonally, taking necessary precautions to ensure privacy of data via encryption and such would be ideally ethical.

When it comes to legal concerns, as long as the cameras only capture things in "public view", there are very few. While some states have restrictions on recording audio of people without consent, as long as you can only be seen while in "public view", it's pretty much all good. When doing research here, I thoug of another use that could be police oversight as the eternal question is who watches the watchmen, that could be us. The opting in approach would also solve the children issue, which is about the only seriously legal obstacle to viewing of public areas.

For Social issues, as always when it comes to powerful technology capable of tracking people we must prevent sky-net and not be evil. This is a number 1 concern. So, to avoid this I think it comes down to choosing customers (if any) very carefully. Or in the case of "do not deploy" policy, avoid the skynet issue entirely.

Anonymous 2713
04/10/2014 11:30 PM

Only thirteen states explicitly prohibit the use of cameras in private places, there are 37 more states that do not explicitly disallow it generally video recordings are legal unless they are explicitly prohibited. There is a large social issue due to the un-easyness of people's recordings and what

[no notes on this page]

companies can do with the recording and the data, ethically Kantianism would disagree with this because the peoples recordings would most definitely be used as a means to an end.

Anonymous 2713
04/10/2014 09:14 PM

PROFESSIONAL ETHICAL LEGAL AND SOCIAL ISSUES AND RESPONSIBILITIES
In order to fully discuss this topic we will take a journey through the code of ethics referenced in the book. The first principle is public: Software engineers shall act consistently with the public interest. However what is in the publics best interest? A conundrum such as this is at the heart of the issue, what do we want as community. The principle 1.05 states we must cooperate in efforts to address matters of grave public concern caused by the software, mass recording of pub places with a technology to identify and store data on the recordings would be according to me a grave public concern. The second principle is client and employer: Software engineers shall act in a manner that is in the best interests of their client and employer. 2.03 states: Use the property of a client or employ only in ways properly authorized and with the client's or employer's knowledge and consent. Some may say a person's face is their own property or their information or likeness is their own property and as a person being recorded they are the client. With these two principles we can safely assume that there ma be a conflict with the code of ethics.

Anonymous 2708
04/10/2014 11:08 PM

There is some discussion about whether the information from this web system should be sold or what the law enforcement has the right to have access to we can look at the code of ethics. 1.04 says that we have the responsibility to disclose information to the appropriate authorities of potential dangers which means that we need to have a system to get information to the police whether we turn it over voluntarily or allow them to access information with a warrant.
Switching to what Nick talked about above we can look at 3.13 which talks about using "only accurate data derived by ethical and lawful means" which can support gathering data in public spaces, using an opt-in system to protect children etc.
When working with facial recognition 3.14 comes into play because we muse maintain data integrity so being able to fix misidentification, changes in appearance due to age, etc. This is important because people change slowly and if data is not kept up to date images of a person at 20 will be unlikely to match those at age 60.

Anonymous 2705
04/10/2014 11:26 PM

As has been mentioned, there is a concern about the security of the information that would be pertained. I however don't see an issue as long as the company stands to [1.01] (Accept full responsibility for their own work) and [5.02] (Ensure that all software engineers are informed of standards before being held to them). Given the proper foundation, the responsibility to security I believe falls within a reasonable line.

Anonymous 2729
04/10/2014 11:48 PM

Haha you and Nick chose the same topic. I agree with Andrew that as long as the company takes responsibility for any screw ups and makes sure to run a tight ship they should be okay ethically insofar as security is concerned.

Anonymous 2705
04/15/2014 02:05 PM

POLICY STATEMENT

From our discussion so far, it is clear that we all have concerns about the potential violation of privacy and overall legality of this product/service now and in th future.

Regardless of the end we come to, it is important that we apply the code of ethics were possible.

Anonymous 2708
04/16/2014 02:23 PM

Looking at ethical code 3.13, which talks about using "only accurate data derived by ethical and lawful means", we can reasonably support gathering data in public spaces because there are no clear laws against it. Kant may say there should also be an opt-in system for any person we consider a child in order to allow parents to give consent so we are not considered to be using children as a means to an end (such as building data).

Anonymous 2729
04/17/2014 03:07 PM

I'm not entirely convinced that Kant would draw the line at children. I honestly feel like all individuals we be used as a means to an end equally regardless of age. I honestly don't think this is going to be ethical by Kantianism no matter what way you spin it.

I would like to once again point out that we can develop this technology, profit from it, and do so completely ethically as long as we don't actually sell it to anyone or use it ourselves. Instead we can just develop a patent profile that allows us to generate revenue by suing the pants off of everyone else who attempts to develop. This is what I am calling the "Ethical Patent Troll Solution" that me and Nick developed. I'm going to continue pushing for this because I feel very strongly that this is the only ethical way to deal with this technology assuming that developing it is required as part of the project assignment.

[no notes on this page]

Anonymous 2703
04/17/2014 04:47 PM

I think if we are not going with the "ethical patent troll solution", and using an opt-in approach it needs to be opt-in for ALL people to be consistent with Kantianism. In developing this product we run into an issue with 2.07. "Identify, document, and report significant issues of social concern, of which they are aware, in software or related documents, to the employer or the client.". I think a skynet type surveillance situation is of great social concern, we must address and report that this is an issue. If this product is deployed at all optint

Anonymous 2703
04/17/2014 04:47 PM

*opting in is the only ethical approach

Anonymous 2713
04/17/2014 08:27 PM

I agree with Nick, we cannot stop companies putting cameras where they can legally put them but if we develop the software to only allow collection of data through users that allow us to collect it, the users could send us a decent portrait of their face that we can match it to and we would have to have to have a minimum match score to not allow false positives, which would follow the lines of 1.4 and 1.5. By making it an opt in approach 1.7 would be followed easily. If we are completely explicit with our business practices and what our product can and cannot do then I see no issues with the software, as long as a user has to opt in to it.

Anonymous 2713
04/17/2014 08:27 PM

I agree with Nick, we cannot stop companies putting cameras where they can legally put them but if we develop the software to only allow collection of data through users that allow us to collect it, the users could send us a decent portrait of their face that we can match it to and we would have to have to have a minimum match score to not allow false positives, which would follow the lines of 1.4 and 1.5. By making it an opt in approach 1.7 would be followed easily. If we are completely explicit with our business practices and what our product can and cannot do then I see no issues with the software, as long as a user has to opt in to it.

Anonymous 2729
04/17/2014 08:41 PM

If we are going to do this then yes I agree it needs to be an opt in situation. That being said how do we feel about anonymized demographic data? For example say a company wants to see where in public women tend to congregate at 5:00 PM on saturdays, is that considered okay? We aren't reporting any specific information to advertisers, just types and quantities of people. I feel like that could be less of a serious issue.

Anonymous 2708
04/17/2014 09:32 PM

I think anonymous demographic data would be ok because we are not doing anything the government doesn't already do with the census data, although we would be making assumptions based on video of race, class even gender in some cases. But with the opt-in we could ask for this type of data to go with their profile, but I am not sure if this goes beyond the scope of what is ok to do.
From what Mike said today in class in the public space there isn't much of a right of privacy so I think at least placing the cameras out and about wouldn't be illegal and therefore ethical by social contract theory.

Anonymous 2713
04/17/2014 10:27 PM

If the users opt in then the data collected would then most likely be available for demographics by the company that owns the software, this would have to be included in an end user licensing agreement. I do not think it would be invasive as the census data, ie. going door to door asking how many people are in your house, but just tracking your whereabouts with consent. Such as amazon's purchasing suggestions, customers who also viewed this bought this could be implemented and be an asset to those who opt in to this service. A situation like this could be in a mall where they track what stores you go in and where you spend the most time and suggest new stores. As long as the anonymous data being used is described to the customers I see no issues with this under the ACM code of ethics.

Anonymous 2703
04/17/2014 10:37 PM

I agree with the ethics of anonymized demographic data. It seems inline with current practices used to improve advertising. It seems we think this technolog would be best used as an opt-in social network type situation or for market demographic research. Using both could provide incentives to join the service, like if you go to a store in the mall alot, you get coupons. Also, i don't think we would need to place any cameras ourselves, as many cameras of public view already exist and our product could be sold to malls/organization of businesses to be used with their infrastructure.

Anonymous 2703
04/17/2014 10:37 PM

I agree with the ethics of anonymized demographic data. It seems inline with current practices used to improve advertising. It seems we think this technolog would be best used as an opt-in social network type situation or for market demographic research. Using both could provide incentives to

[no notes on this page]

join the service, like if you go to a store in the mall alot, you get coupons. Also, i don't think we would need to place any cameras ourselves, as many cameras of public view already exist and our product could be sold to malls/organization of businesses to be used with their infrastructure.

Anonymous 2729
04/17/2014 10:42 PM

@Sarah Can't you just not respond to the census? It seems like in our system people don't really get to opt out of anonymous data collection.
@Bryce I certainly think that we could give users enough of an incentive to be tracked that we could convince them to opt in, just look at Google now, you have to opt into to google's search tracking for the feature to be enabled but people love it regardless.
@Nick I agree, it certainly seems like we could structure this to end up with the highest net benefit to both customers and companies through targeted ads.

Anonymous 2708
04/17/2014 10:43 PM

So what about polices concerning the prompt software web cam history (or whatever it is called) in terms of that software we do an opt-in and use the information solely for demographic research and targeted advertisements as a way to use it in an ethical manner? Also, any thoughts on law enforcement rights to our information, videos etc.

Anonymous 2705
04/17/2014 10:53 PM

There is certainly a need to structure this in a way that follows the code of ethics. In light of the conversation today with Mike Gaffney, what is legal for us to do, doesn't necessarily fall under our ethical obligations. There is not always a clear definition of privacy, especially when it comes to public property.

In the event that we were providing a service of anonymized demographic data, I would say that yes it is very reasonable to supply the information to companies, private citizens, and the government. Hitler used unanonymized demographic data, and look what happened there.

Anonymous 2708
04/17/2014 11:37 PM

So unless we put making the webcam software public in our opt-in system it probably shouldn't be public, I think if we work out act utilitarianism the cost or cons to the public does not out way the potential usefulness of this software being public. Also in terms of how we would make contracts to use cameras owned by private companies (assuming we are going to) we would probably not want to give access to the webcam history software but I guess we could potentially trade our anonymous demographic data in exchange for the use of their cameras. For law enforcement I guess we would apply with warrants (due to social contract theory) but we wouldn't just hand over information without one.

Anonymous 2713
04/17/2014 11:47 PM

We could also make a rule that anytime you are being recorded there has to be a visible sign or posting that explains why and how your recording will be used. I believe that would be a good thing to include in our user agreement. And would overall lead to a better society.

In respect to law enforcement depending on how much data we collect and use most of our stuff could be encrypted and could be limited to only the software to dissuade "wire tapping" the act of a warrant though would lead us to provide access to whatever evidence we can view, however I do believe nobody thinks warrants are a bad thing. Warrant less searches and seizures however..

Anonymous 2729
04/17/2014 11:48 PM

Way to Godwin this conversation Andrew geeze.

Anonymous 2705
04/17/2014 11:52 PM

Alright, let's say we were to only use cameras privately owned and made sure that any unanonymized data were released under warrant. I feel that this would be a major step into a SCT acceptable arena. I don't see a problem in using company owned web cams, as our software would most likely be in a closed box somewhere not on the camera.

[no notes on this page]

Appendix C:

Committee Members' Ratings, Justifications and Deliberations for Each Discussion

Ananth Kalyanaraman
07/01/2014 05:55 PM
Chris,

Please find my updated ratings. Hope this helps.

****
Team 1:

Criterion D: Change my new rating to 2.0 (needs improvement).

Notes: I was probably too critical initially. But I'd still not put this team in the capable range for this outcome.

Criterion F: I prefer to keep my rating as is at 2.0.

Team 3:

Criterion F: Change my new rating to 3.0 (capable).
Criterion G: Change my new rating to 3.0 (capable).

Notes: My old ratings must have been an entry error.

On criteria H&D, I'd like to keep my current ratings unchanged.

Team 4:

Criterion D: I'd like to change my new rating to 2.5 (between needs improvement & capable).

Notes: I think the discussion, on second reading, did demonstrate the ability to function a "team".

Criterion F: Change my new rating to 3.0 (capable).

Notes: again, my old rating here for whatever reason appears to have been an entry error.

Christopher Hundhausen *Instructor*
07/02/2014 03:28 PM
Thanks, Ananth! Carl and Larry, Could you please reply to this thread ASAP with your updated ratings and rationales? Thanks!

Larry Holder
07/02/2014 03:32 PM
I seem to have lost the mapping of team numbers, but here's what I have (original ratings plus changes where appropriate).

Team 03 (35394)
D:3 Indepth discussion by all team members; no clear summary of final policy.
E:4 Good discussion of issues.
F:4 Excellent communication skills by all team members.
G:3 Good discussion of local and global impact.
H:4 Many references to relevant material.

No changes after reviewing other reviewers' comments.

Team 05 (35393)
D:4->3 Indepth discussion by all team members; good summary of final policy.

Christopher Hundhausen *Instructor*
07/02/2014 04:32 PM
Thanks Larry! Carl, could you please send your updates ASAP?

Carl Hauser
07/03/2014 11:36 AM
I really don't see any basis for making changes -- my original ratings justifications are gone and I can't even seem to access the original student submissions. I was confident in my ratings so I'm not going to change them just to make them more aligned with what others said. I remember that many of my scores were in between whole number ratings but those were only in the comments that are now lost so I don't even know which direction I was leaning toward change. Maybe I'm not understanding something about the OSBLE here and you can point me explicitly to where I should look for my and others comments -- Larry seems to have had access to them in making his comments above -- but I'm not finding them on my own.

One thing that I noticed when I originally compared ratings by the CSCC for communications was that I was a lot less strict than Ananth was about colloquialisms -- I thought that in a blog discussion it was OK for students to be informal and did not look negatively on that.