Problem Solving with an Improved Internet – Case Study: Campus Rape

Abstract

Society faces a number of difficult problems that might be solved with cooperative effort. One of these is relationship violence, including rape, on college and university campuses. Recent studies show the problem is widespread and growing. Internet methods like social networking might ameliorate the situation in principle. In practice, they don't. The matter is too sensitive and private to trust to the open and easily exploited Internet. We need an improved Internet that protects secrets while sharing them when and where necessary.

This paper describes why the problem is currently intractable and then explains how the Internet can be improved. The use of the future system is illustrated with screenshots of prototype software.

You can see the future system demonstrated on YouTube:
http://youtu.be/LEcXOPuGzrs

Contents

Why this paper? What is it about?

Society faces many difficult issues. Often, people can improve the outcome when they work together. A problem that is unmanageable for a single individual can be solved with group effort. But, how do people find each other and form alliances? How do rape victims, who fear public censure, band together to obtain justice?

The Internet should play a role. It is ubiquitous and connects people across continents, across generations, and across campuses. Unfortunately, the Internet is not the place to put private secrets. All will be vacuumed up into the "Big Data Cloud" with unforeseeable future consequences. More and more, our personal life is exposed to complete strangers. The time has come to improve the Internet to deal with sensitive, private matters.

Can we improve the network? Yes! I'll illustrate how by focusing on a delicate problem involving violence – campus rape. Maybe you don't want to talk about rape. Ok, but keeping silent about problems will not solve them. I'm highlighting this problem to seek justice for victims of this crime. If I can convince enough people that technology can help here, then there is a chance for progress.

I'm writing this article because I can see a bridge that connects existing technology with new solutions for society's problems. Not everyone can visualize the connection. That gives me an obligation to write this. You can read my qualifications on my LinkedIn page cited in the references.

I hope this message reaches the academic community where bright, innovative, energetic minds can initiate a major change in the Internet. Also, that community has the campus rape problem. For that reason, I hope faculty and student leaders will listen to this idea and back its implementation

Why the Campus Rape Problem Won't Go Away

If a woman is raped on campus, the crime will rarely be reported. Here are some valid reasons why the victim remains silent.

Reason 1: A significant, influential segment of the public blames the woman. For example consider the opinions in a recent syndicated column by George Will (ref. 1). George believes "Washington" (whoever that may be) wants to "make victimhood a coveted status that confers privileges" thereby inflicting irreparable harm on impressionable young men confused by "the ambiguities of the hookup culture, this cocktail of hormones, alcohol and the faux sophistication of today's prolonged adolescence of especially privileged young adults". If your father shares this judgmental attitude, would you want him to hear about what happened to you?

Reason 2: What happened definitely does not enhance your status in any way; moreover, you will find a way to blame yourself. Better to keep quiet.

Reason 3: When you make an accusation, you face emotional and health stress. Your case is unlikely to come to trial. If it does, the judge will be biased against you. While the perpetrator goes free, you are left with hurtful memories. These opinions are buttressed by extensive statistics and surveys (ref. 2). This is why victims keep silent.

You may be thinking: why not post the accusations on a web site anonymously (protecting the victim's privacy) and hope that the perpetrators can be shamed into better behavior or perhaps ostracized? Unfortunately, that online list would encourage another kind of bad behavior. The pettiest grievances could be avenged by posting an anonymous accusation against someone we want to hurt. The victim of the slander has no recourse. Hopefully, this fix will not be tried. For a serious accusation to be raised, the veil of anonymity must fall. It is sensible to maintain anonymity, however, until there is a reasonable, credible case that will stand up in court.

We know from the cases that have been reported that many transgressors are serial offenders. If multiple accusers come forward, a court must take the complaints seriously. However, at the moment, there is no way to maintain anonymity and bring together women who share a grievance. Before we can do an anonymous match, we need to improve the Internet.

Finding Solace with New Allies

No common database of sexual offense reports should be kept. A big, combined database is a tempting target for hackers. It would not be secure. The solution is local and friendly but must be indirect to protect privacy. Prospective users are encouraged to connect with a local group that they trust to keep a small, secure, local database of reports. As a member of a local group, you can report any offenses using a secure login to a computer or smartphone. (For an example, see Figure 1 on page 5.) Your sensitive report is hidden – hidden even from other group members. No information leaks to the "Big Data" cloud.

Your group has several obligations. First, it operates a reporting service just for group members and maintains their privacy. Secondly, it works on behalf of its members to discover other offenses on campus that relate to the experiences of its members. The goal here is to find allies who have a common cause. When potential allies are found, each woman can decide whether to connect, discuss the mutual experience, and choose the next step.

Each group is completely isolated in terms of administration and data security. Nobody can login to a group and compare reports across campus. To find the connections between reports, we need a service that acts as a "blind matching agent". Let's explain that term and how the agent works.

An "agent" is software that works on your behalf but you don't need to run it yourself. Each group has an agent that works for the members of the group. This group agent accepts the report from the users. In addition, there is an independent third party "blind" agent that completes the solution. The third party is "blind" because it receives

only encrypted summaries of the reports. It can't actually read the reports and anyone who breaks into the third party agent cannot read the reports either.

The blind agent periodically checks in with all the agents for local groups. When the agent checks in, the group agents respond automatically by encrypting the reports with a one-time encryption key. Groups send the encrypted reports to the "blind matching agent" – but they never send the encryption key. Now the agent – operating "blind" because it can't read the data – matches the reports and marks sets of reports that appear to refer to the same perpetrator. That is possible technically because a computer can match encrypted values even when it can't convert them to their original name or date or other meaningful fact.

The blind agent sends any matches to the groups that represent individuals. (For example, see Figure 6 on page 8.) The matches arrive encrypted, but the group agent has the key to read the results. Thus, if you submitted a report that was matched with other reports, you will learn how the reports match. You will learn that others are in the same quandary for the same reason. You may decide to work with them. If you decide to go ahead, you allow your name to be shared with fellow victims.

With the Internet working this way, victims can form alliances to go after the perpetrators. Punishing the perpetrators will reduce the incidence of crime. People working together can succeed.

A Tour of the Shared Secrets Process

The users of this shared secrets process are women. Each has access to a secure smartphone app or to a login for a secure web server. The following figures illustrate an app registered to a fictitious woman, Eunice Yearby, who belongs to the Alpha Phi sorority.

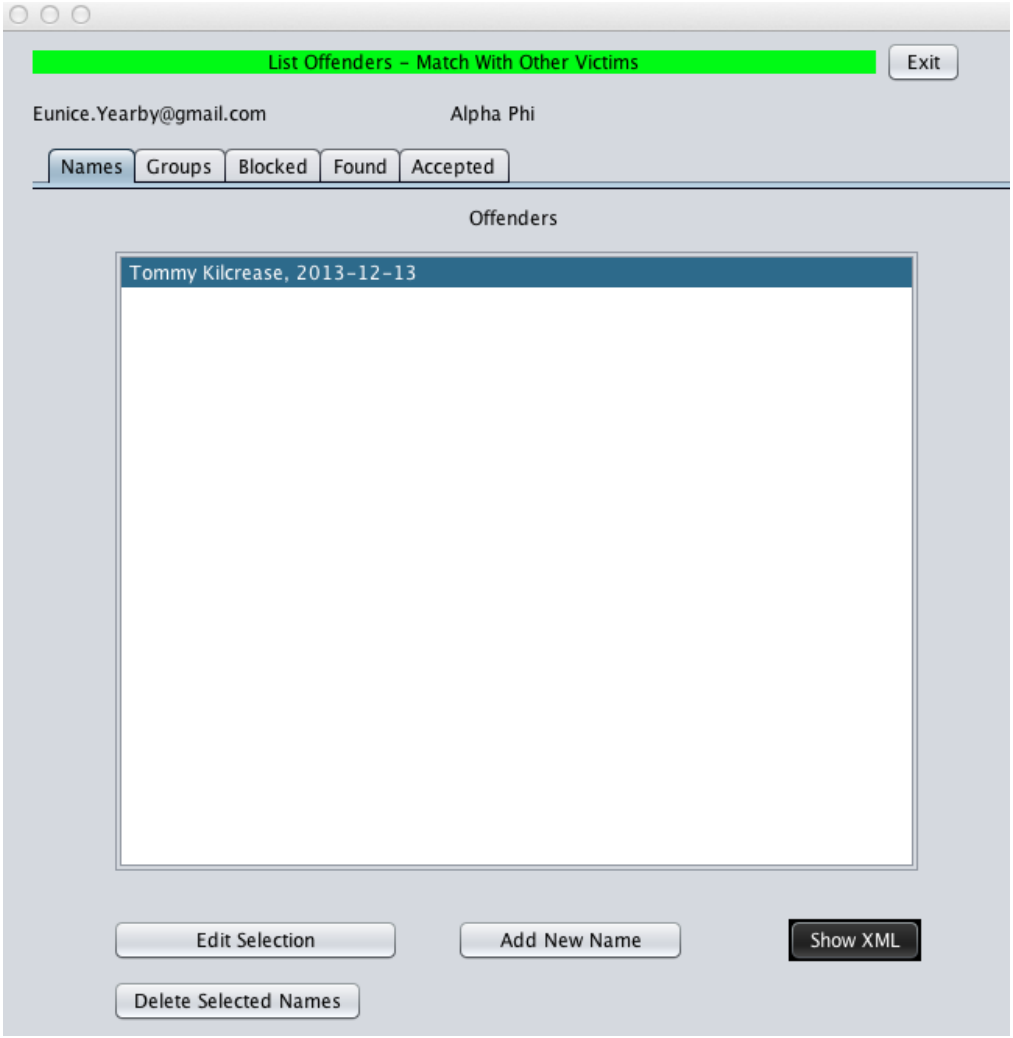

Figure 1: Here is a snapshot for a fictitious woman Eunice Yearby in the Alpha Phi sorority. A fellow named Tommy Kilcrease bothered her last year. He is the only person she has listed. Let's click on Tommy's entry and see the details in Figure 2.

Figure 2: The entry form for offenders showing the details for Tommy Kilcrease. The level of the offense is coded with categories defined on the George Mason University web site. The "Explain" button would take you there.

Figure 3: Eunice has been watching for any other reports about Tommy by clicking on the "Accepted" tab in the application. As we see, it is currently empty. While she is waiting, Eunice is protecting her privacy as we see in Figure 4.

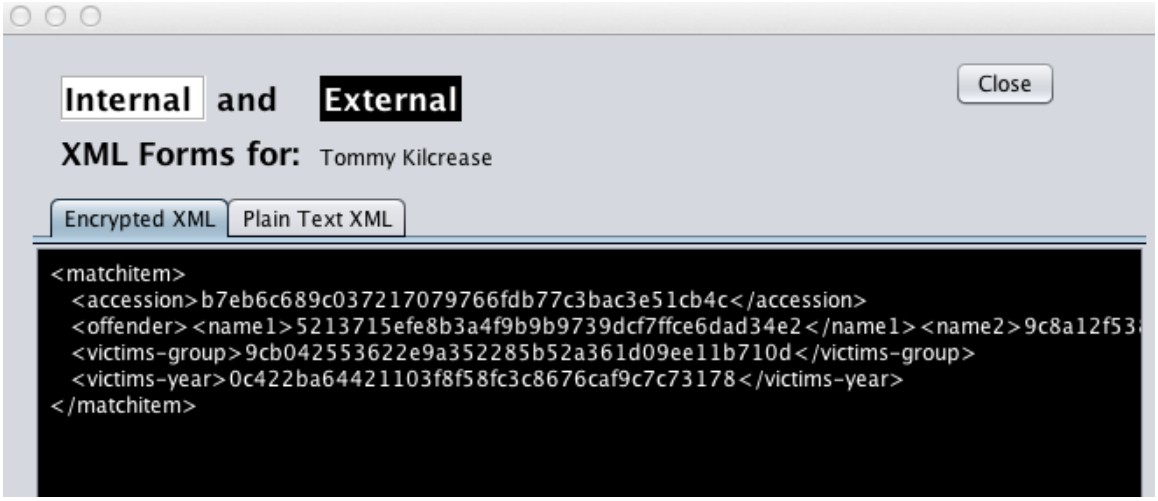

Figure 4: Encrypted record for Tommy Kilcrease. The encrypted record is the only thing that is shared with the campus-wide matching computer. If hackers get in there, they are unable to use the names or dates. Incidentally, this illustration uses a "baby" encryption algorithm. A realistic algorithm produces so much random looking output that we could not illustrate how the encrypted fields are flagged with tags (e.g. the <offender> Tag).

The reports that women file are held securely and locally. It is much more secure to hold small amounts of sensitive information in many distributed compartments. Because compartmentalization prevents anyone from discovering related reports, a temporary encryption conceals the report so that it can be safely shared with an encrypted matching agent. In a production software system, the user would never see encrypted reports, but the demonstration software includes an illustrative display shown in the next figure.

When Caroll Loden arrived on campus she joined the Kappa Alpha Theta sorority and, on the sisters' advice, registered for the system. She's been enjoying a safe, engaging learning experience so far and her screen for "Names" is blank. In fact, she has almost forgotten the system until she meets Tommy at a party.

Now Caroll has met Tommy, her attitude towards campus life is becoming one of fear and trepidation. In fact, fear is making it hard to learn. So she seeks support from other women with the same experience. The app lets her enter some details about her recent experience with Tommy. She clicks on the "Add New Name" button on the "Names" Tab as illustrated in Figure 1. She can then enter details as shown in the Figure 5.

Figure 5: Caroll's report about Tommy Kilcrease. When she saves this report, it appears in her report list; moreover, the encrypted version is shared with the campus-wide service.

Figure 6: Caroll Loden's encrypted report has matched the earlier encrypted report from the Alpha Phi sorority. Caroll sees the match in the tab marked "Accepted". When she clicks on "View" she will see more details as shown in Figure 7.

Figure 7: The match result was computed completely in encrypted form to protect the names but Caroll sees it after decryption in plain text If Caroll decides to contact Eunice, she can send a secure e-mail message via the app by clicking the button.

Of course, on the other side of campus, Eunice Yearby will learn about Caroll Loden's bad experience the next time she opens the app. For Eunice, this will be news that she is not alone. In many real-world cases, we may expect to see three, four or even more matches on one offender's name. This system helps single out repeat offenders so they don't pollute the spirit of campus life.

Now over in the administration building, the Deans may be denying there is any problem. This system will not present them with any names, dates or facts unless the victims decide to come forward. On the other hand, the matching service can still count incidents even if it can't read the incident reports. If the administration asks for it, it can receive a report like the one we show in Figure 8.

Figure 8: Sample report from the campus-wide matching agent. Although the agent cannot read any details of the reported incident because they are encrypted, it can count. The counts of incidents may help engage the interest of campus administration.

These illustrations are derived from prototype software that you may also see demonstrated on YouTube. See Reference 4.

Summary

We have seen how an improvement in Internet facilities could allow people with similar concerns to find each other anonymously without revealing personal details on the web. Once they find each other, they can form an alliance and move forward as indicated by facts and circumstances. The service described here could be deployed on campuses to aid victims of sexual offenses.

The service does require a significant improvement of Internet software. The effort, however, will be justified by the serious issue discussed here and by other applications that require both data privacy and selective, mutually-approved data sharing.

Author's Contact Information

Dr. Paul L. Baker

Email: pbaker@wwnsoftware.com

LinkedIn: http://www.linkedin.com/in/pbaker1/

Blog: http://ectn.typepad.com

References:

1. Editorial by George Will, Washington Post, June 6, 2014: *Colleges become the Victims of Progressivism*. http://www.washingtonpost.com/opinions/george-will-college-become-the-victims-of-progressivism/2014/06/06/e90e73b4-eb50-11e3-9f5c-9075d5508f0a_story.html

2. See, for example:
   Editorial by US Senator Claire McCaskill, *Universities failing to protect rape victims*", http://indy.st/1maBT9y
   also:
   the article by Tyler Kingkade, *Prosecutors Rarely Bring Charges In College Rape Cases*: http://www.huffingtonpost.com/2014/06/17/college-rape-prosecutors-press-charges_n_5500432.html

3. White Paper: *A Scenario for Responsible Information Sharing with Sensitive, Private, or Classified Information:*
   http://www.wwnsoftware.com/pdf/scenario201207.pdf

4. *Connecting Secrets to Ameliorate the Campus Relationship Violence Problem*, YouTube: http://youtu.be/LEcXOPuGzrs