Privacy Considerations for Radical Communications Systems

For many people, it's a strange notion that an online service provider would ever care about the privacy or security of their users. Taking a quick look at the top 10 most frequently visited sites in the world[1], nine of them have based their business model off the accumulation of private information for the purposes of targeted advertising or sale. The exception here is Wikipedia and this speaks to the way the ethics and goals of an online service provider play into how they treat their user's privacy. Wikipedia is a non-profit that doesn't rely on advertising money or detailed information on users to turn a profit, they rely on community support to keep their website online. Even with the example of Wikipedia, they do log personally-identifiable information about their users such as IP addresses and in some cases, store the information indefinitely.

For people involved in social movements, there is a higher awareness of the need for online service providers to protect the privacy of their users. As participants in social movements, they are targeted by government agencies, corporations, and other adversaries simply for their political activity. Somebody is always wondering what they think, who they know, how their money is spent, what websites they frequent, and so on until the most intimate and private details of their lives are transcribed and stored somewhere.

Radical service providers such as Riseup Networks and Indymedia have had a long-standing policy of respecting the privacy of users by limiting the retention of personally identifiable information. They do not log IP addresses or other types of information and when they do, they make clear what they are logging, why they are logging it, and how long they will retain it. They have these policies to protect against clearly defined adversaries who want to harass, intimidate, and neutralize people in social movements.

For providers of radical communications services, privacy and user consent is also a key consideration in designing their systems. Users of these systems are likely to be protesters, journalists, and everyday citizens who do not want the government knowing about their activities. In the past, we have seen several efforts to raid communications centers during social crisis and seize electronics. In every instance, members of the communications teams were arrested under vague pretenses so law enforcement could gain access to what they presumed to be large troves of data on the users of these services. Unfortunately for them, the communications software was configured to not retain this information.

Communications services operate entirely through a network that is controlled by, monitored by, and actively disrupted by forces that do not care about free speech, access to information, or the lofty ideals that operators and users of communications services often have. They, in fact, have the complete opposite goals: profit, stability, and compliance. For this reason, operators of radical communications services must cleverly use technology to thwart attempts to harm their services or users.

All radical communications systems will have different goals for their services, but these privacy goals should be taken under strong consideration.

Do Not Ask for or Retain Personally Identifiable Information

The easiest way to insure the privacy of your users is simply to never ask them for or retain personally

identifiable information. This includes IP addresses, referrer addresses, phone numbers, or anything else that is not absolutely necessary for the successful operation of the system.

For information that must be retained, establish a clear method and timeline for purging the information when it is no longer needed. When it is purged, securely wipe the data instead of just deleting it.

Fully Encrypted Data Storage

It is inevitable that some information will be stored unintentionally and that some deliberately stored information does not need to be retained for a long period of time. In the case of personally identifiable information, it may be that certain information (such as the phone numbers of independent reporters) may need to be stored temporarily. If the equipment storing this data were to be seized and that data had been stored on it, even if it had been deleted, it could be recovered. For this reason, data should never be written to a disk unless it is encrypted. If the data is encrypted, recovery efforts may be successful but the data will not be able to be decrypted unless service operators hand over the private keys/passphrases. Systems like Truecrypt (Windows, Linux, Mac) or luks (Linux) work well for this.

An even better solution for this problem is to simply never write anything to the disk. Instead of pre-configuring systems that are installed on the operator's computers, it makes more sense to simply use LiveCDs and then configure the computers from there. This allows short-term storage of data without ever touching the hard drive and the data would be almost impossible to recover once the computer is turned off. In this situation, not even the operators of the system have the ability to hand over any personally identifiable information that had been stored.

Encrypted Transport

In the same way that you encrypted stored information to keep it secure, you also want to encrypt that information in transport . The best way to do this is to encrypt the data between your servers and the users. Depending on the setup you have, you can do this through SSL/TLS or VPN protocols.

Secure by Default

If users have to perform additional work to receive security, there is a good chance that they will not do so. This is partly due to widespread technical incompetence, fear or uncertainty with changing settings on their systems, or not understanding what the security you offer can provide them or other users.

Since you, and the individual user, don't know the security needs of every user, it's important to assume that all users require the highest level of practical security. For this reason, when a user connects to your system, their connection should be encrypted by default, you shouldn't store their information by default, and the tool they use to join your communications system should be designed with similar privacy concerns in mind. If users desire less privacy (for instance, if they want you to know who they are so they can submit information without needing extensive verification), there should be a clear route for them to act on that desire which adequately explains what additional risks they are taking.

1. http://www.alexa.com/topsites