Not That Kind of Friend
(Transcript of Discussion)

Jonathan Anderson
University of Cambridge

It falls to me to deliver the last talk, so I’ll try to keep you all awake.

We have this idea of social networks in the real world, and then there’s this thing that we do on computers: they use some of the same language, syntactically they might be similar, but semantically they’re completely different, and this leads to a lot of really appalling things.

Frank Sta jano: Our group has been fairly active in exploring the security and privacy of social networks, and this is something where the old hands, like us, don’t really understand what goes on. We were discussing yesterday with Matt, what is there in such a network that you can’t do it just by having your own webpage? We don’t get it, so we need some fresh blood, and this year we have had a good influx of smart people who are young enough to understand this stuff and have been using it since they were in college, and who, from the inside, can find so many holes. So this is an exciting time for this kind of exploration.

This is the last talk of a workshop where you are supposed to interact, so we do encourage you to interrupt as we go along. This is a topic that, as we have seen from the previous talks, resonates with many people; many of the issues that we want to bring up are things that people have been mentioning, so do chip in with your ideas. This is not about delivering received wisdom to you.

The problem that we are facing is that privacy issues in social networks, which stem from many things that are done in a appallingy poor way, not least of which is the choice of words even to describe what is being done, and what the social network people say they do has little match with the ordinary meaning of those words. So maybe what we seek to get out of this discussion in this last session is some clarity.

Reply: Everybody is aware of social networks at this point, no need to talk too much about them, they’re popular with millions of people, and multiple social networks are ridiculously popular, and they’re everywhere. They are becoming an essential part of the infrastructure of a lot of systems, so Facebook Connect is now the arbiter of identity on the Internet. Facebook says you are Bruce Christianson, therefore you are Bruce Christianson to the New York Times, and to whoever uses Facebook Connect, which is a lot of people. And of course there’s been some pretty appalling privacy problems.

Bruce Christianson: What do you mean by privacy in this context, or are you just about to take a little bit of the wrapping paper off.
Reply: I’m talking about people’s expectations. I’m going to define some terms a in a few minutes, but people’s expectations aren’t being met, basically. The first question is, who cares? People say, well you know, you’re putting all this stuff on a webpage so you deserve whatever happens if anybody looks at it. Well, you might think that, but people really do have this expectation of privacy, and if that was all that there was to it, then you could chalk it up to people being silly. But in fact, social networks go out of their way to say, no, no, no, we give you control of your information, so if people are making promises like this then maybe we should build systems that can actually fulfil the promises. So people have this expectation of privacy, and we say, well are these things really important, I mean, who cares if anybody sees it.

Well there are real adversaries out there who are looking for lots of different kinds of personal information, and there are real threats, and we’ve seen things like people getting fired, and employers surveilling their employees, even if they’re not necessarily firing them, they’re still introducing weird things into the corporate culture. There’s phishing that’s going on, and there are blackmail things as well, at least one or two that we know about, but who knows how much blackmail is going on that we don’t know about because that’s kind of the point. And there’s lots of frauds going on, the whole, help I’m lost in London with no money, please send me $900, thing.

We say that privacy is a problem, so what is the problem? These two categories divide into the two different definitions of privacy. On the top we’re implicitly trusting the operator, this pertains to data protection stuff, my relationship with Facebook and all of the entities that are associated with Facebook. And the bottom is the access control side, which is more related to the personal privacy, my information getting out to friends, to people that I don’t know, that sort of thing. So we contend that there are two big problems with the way that privacy is done in social networks. First you have to trust Facebook implicitly, and second, the access control mechanisms that are in place are quite silly.

So you’re trusting the social network operator, you have to trust them completely, you give them all the information they could ever want to walk into Barclays Bank and say, hi, I’m Jonathan Anderson and I need to change my chequing account number, or whatever, and you give them all this information about personal relationships, which can be used to do really good phishing. If you can drop a few friends names into an email and make it look like it came from one of your friends, phishing rates go way up, so there’s a lot of information here which is really sensitive. And the other thing is, you’re not just trusting them completely with everything that you have, you’re trusting them absolutely because there is nothing that you can do if some random Facebook application developer runs away with all of your data and sells it to somebody who wants to commit fraud, there’s nothing you can do about it. But furthermore, there’s no alternative, right, the only legitimate alternative to not trusting Facebook, MySpace, whoever the centralised provider is, is to just not use social networking. Some people say, OK, fine, I’ll just not use social networking. But there are