

Thursday, October 25, 2007

Web 2.0 p... contest

Waves of adoption are a really interesting thing. Especially in regard of Web 2.0 services. From time to time such a wave goes through an organisation and many people register to such services without really thinking about it. Such a wave was induced by a weblog entry of James Governor by touting a contest of IBM and Sun about the adoption of dopplr.

Dopplr is a service to share your travel plans in your peer group. So you can look up, which colleagues are in the same city. Now, before i get to my doubts about such "Where I am" services, there is a more general question: About the "Qui bono" of such a pissing contest. Well ... it's a service without an compelling use case. When i'm travelling to a city, i simply look into the calendars of my colleagues or send them a sms. I don't need a service for this. And to say it frankly: I don't meet with people for a drink just because of having the same company name on the business card.

Albeit Web 2.0, communities and social networking are nice things, they should have a clear advantage. And i don't see this advantage in dopplr. So .. of what avail is this contest: Maybe only many new users and validated email adresses for dopplr ...

My primary rant about such "Where i am"-services is not specific for dopplr. It's the same problem with services like plazes.com. You give away a very sensible part of data about your life and possibly the life of others: "Where are you at a certain point of time?" The answer to this question answers a more interesting question: "Where are you not at a certain point of time?". For example: Not at home. And this is an interesting answer for some shady businesses, like freelance possession transfer aka larceny.

You have to answer some questions to yourself when you sign up for such a service:

Do you trust the provider of the service? E.g.: It's data protection policies, their practices in handling data, their practices in handling their backups ... Do you trust the security of the software? E.g.: There was a problem with a large community portal in Germany allowing everybody to download the profiles Do you have enough physical (locks, CCTV, alarms) or organisatorial (insurances) protection to cover the increased risk. And as high qualified workers tend to earn more money and tend to have rather wealthy peer group, even the usernames and passwords of Sun or IBM employees for dopplr gathered by trojans or security leaks may be quite useful.

In the end this may be a little bit paranoid. But only because you are not paranoid, this doesn't mean that they are not after you.

Posted by Joerg Moellenkamp in Business Travel at 13:28