Presenting choices in context: approaches to information sharing

Jonathan Grudin and Eric Horvitz
Microsoft Research
jgrudin@microsoft.com and horvitz@microsoft.com

We are exploring the nature of people’s reservations about information sharing and potentially intrusive notification, and experimenting with designs to address concerns. Thus the “boundaries” are for what goes out, what one is willing to share, and what comes in, what one is willing to be interrupted by. These have different dynamisms and other properties. Below are several examples that illustrate work at different stages of development.

Concerns about sharing information
Interviews are frequently used to identify people’s preferences in sharing information about themselves or the objects such as documents on which they have worked. As noted by Chris Nodder in his submission, interview subjects may not be able to access or recreate enough context to understand how they will actually feel in real situations. He observed behavior and determined that it was often inconsistent with self-reports. We have taken another approach to mapping out this space, collecting specific examples of incidents where someone was reluctant to share some information or object with one or more other people. We have collected a large number of such incidents and provisionally categorized them. The figure below is a first cut at identifying the range of reasons people feel uncomfortable sharing. Our plan is to extend and refine this list, which can be used to identify possible issues and features for information-sharing and notification systems.

Approaches to access control
We have built here on the discussion of optimistic and interactive alternatives to the standard pessimistic access control as outlined by Povey and illustrated by Stevens & Wulf. In pessimistic access control, privileges are set before someone can access the information, which could be an object, status information, personal information. This is the most common, and of course there are good reasons for doing it. But there are some problems. People don’t want to fill out complex forms describing differences in privileges. Also, privileges must be set when the object or the information is created, and at that point you may not know exactly who you will want to see the object, who will need to access it, and so on. So you may set it too conservatively or too loosely. And exactly who should get access changes over time, and people often don’t take the time to adjust privileges.

The opposite approach in some ways is called ‘optimistic’ access control. You let anyone access the information, but you monitor and record who accessed it and when. There is a natural quic pro quo – you are allowing greater access, in exchange for which the viewer agrees to the logging of access. This approach does imply a relatively closed system, that
you can identify the people coming in. You can review the log and revoke someone’s ability to access the information subsequently. Of course, this won’t work for information that once someone sees it or gets a copy, the cat is out of the bag. But there are cases where optimistic access control could lead to useful sharing.

A Microsoft example is calendar information. At Microsoft, almost everyone shares only free/busy information. But there are organizations where people voluntarily share all of their calendar information, except maybe a medical appointment or something blocked off as private. It can be extremely useful to share detailed calendar information. You’re busy from 1 to 2, but if I can see the details, I know where you are – will you be in your office at 2, or in some other building. Or I can tell if this is a meeting you are really likely to be attending, or one that’s in your calendar but you’re likely to skip it. Or is this an important meeting with 5 other people, or just a meeting with a colleague that you could probably reschedule if there’s a conflict. People use calendar information all sorts of ways when it is accessible.

So, why don’t people use open calendars at Microsoft? If you ask, the primary reason is concerned about micro-management -- viewing by their manager, a higher-level manager, or possibly someone else. With optimistic access control, you could experiment: Open your calendar for a week, log who accesses it when, and at the end of a week check the log. You look and if… your manager is checking your calendar 5 times a day… end of experiment, end of access, calendar closed! But this isn’t likely, managers are too busy for that, more likely you’ll find your calendar was accessed a couple times by people trying to coordinate with you. So you let the experiment go for a month. Then you check and find pretty much the same thing, but maybe there is this one person who occasionally checks your calendar and you don’t know why, so you can block access for that one person, but let others in.

The third approach to access control is potentially the most interesting. In interactive access control, when someone wants to access information, a request is generated, you get the request, maybe in real time if you’re at your desk, or asynchronously otherwise. And you have some simple options – grant unconditional access, grant one-time access, deny access. The interesting thing about interactive access control is that it provides a way for users, and perhaps the system, to detect a pattern in behavior, to decide how you feel about granting access at the moment you are thinking about it. For example, you create a document and you aren’t sure who you might want to share it with, so you put it on interactive control. A request comes in, you grant it. Another request comes in, you grant it, and you decide that you feel comfortable sharing this information, so you make it freely accessible, and maybe check later to see who is accessing it. Another document, a request comes in, you deny access. Another request comes in and you think, you know, I’m really never going to feel comfortable about sharing this, so you block all access. A third example, the system notices that over the last couple weeks you’ve received three requests from people in this particular other group and you’ve granted them, so the system says “would you like to open access to all members of this group?” since there seems an acknowledged need to know. So interactive access control gives you the ability to modify your access privileges after you’ve had some experience with the object, at the
time you’re thinking about your comfort level with sharing, hopefully with a simple button click or two. (For an ad hoc or system-identified group, the set of group members could be presented for verification and editing, possibly even indicating which members had accessed the information.)

All three models are implemented in a fashion in parental controls. Of course, it isn’t the web site owner that decides whether or not the child can access the information, it is an intermediary, the parent. Parental controls can be exercised pessimistically – the child can’t go to these sites. It can be implemented optimistically – the child can access anything but it is logged and can be reviewed by a parent. It can be interactive – content of a certain kind can only be accessed if a parent approves. Refinements are possible, such as opening access for a specific period of time – while working on a report on breast cancer, control would be relaxed, but after a week, no more breasts. This diversity of approaches to access control could be useful in a broader range of settings.

As we have worked on a prototype implementation we have found that the issues surrounding these approaches get more complex, and we can talk more about the additional dimensions and considerations that emerge.

So these are the kinds of issues we’re exploring, along with other aspects or dimensions. Identifying natural groups of people – colleagues, family, members of a distribution list – to simplify setting privileges for different kinds of information – financial information, medical information, family events, and so on. Is trust transitive – would you trust the people trusted by someone you trust very highly? And so on. (Also Figure/Quadrant 3.) A key challenge is whether this can be presented to people in an understandable, manageable way.

Figure deleted to meet email length limit.

The figure above provides an overview of some of the issues addressed by the system and the information owner and requestor. The figure below provides examples of designs that explore different forms of trust and access.

Figure deleted to meet email length limit.