Ethic of choice for Location based systems

Implications, lessions and failures

Mika Raento

Basic Research Unit, Helsinki Institute for Information Technology
Department of Computer Science, University of Helsinki
Mika.Raento@cs.Helsinki.FI

1 95/46/EC and the ethic of choice

As location-based services implicitly tread on data people consider private, they always demand not only techical and design decisions, but *moral* decisions as well. The basic texts that we normally use for making these moral decisions are the EU directives 95/46/EC ”on the protection of individuals with regard to the processing of personal data and on the free movement of such data” [1] and 2002/58/EC ”concerning the processing of personal data and the protection of privacy in the electronic communications sector” [2] (and their national implementations at each member state). These documents reflect strongly the underlying *ethic of choice* that is the basis for the existence and legislation of the EU, and consequently so do our decisions based on these documents. Implementing the underlying ethos is not as simple as following the letter of the law though, and there is even some question as to whether that ethos reflects users' motivations and preferences. (In the following I mainly focus on 95/46/EC and its terminology, as conceptually I feel that 2002/58/EC is just an interpretation of 95/46/EC in relation to data communications.)

The theoretical framework of ethics of choice boils down to a fairly simple idea: A choice is morally correct, if it puts *minimal constraints on other people's ability to make choices for themselves.* This idea is carried through in 95/46/EC in the provisions that the data subject should be able to know the extent of data collection and the purpose of collection and processing before engaging in an activity that implies consent, and when such an activity does not exist, the directive requires explicit consent. The main purpose of the directive is thus to allow data subjects to make an *informed choice.* The other provisions of the directive can be seen to mainly be there to support this main purpose.

The idea of informed choice contains two words, both crucial to its understanding. *Informed* means two things:

1. The data subject has to know that there is a choice to be made. In the case of the directive, this mostly means that people should be aware of the existence of the directive itself.
2. The data subject has to know what the consequences of the choice are. This is provided for in the directive in that the controller has to provide information

about what data is collected and what it is used for. The controller may not decide unilaterally to reuse the data for something else.

The word choice should probably be elaborated into *true choice*:

1. The data subject should have a *clear opportunity* to make that choice
2. The data subject should be *willing* to make that choice
3. The data subject should be *capable* of making that choice

Unfortunately, although the law is often followed to the letter, people are not making informed choices. There are several obstacles on the way, that have interesting implications for system and user interface design.

2 The users are not making the choices

Most users do not care about what happens to the personal data they give out [3]. They do not request to see information of the registries data is put into, and even if they receive such information they do not read it. This is true for traditional data collection activities, such as companies' customer databases, as well as consenting to transfer of location data to value-added service providers. If we pop up a long text on a small mobile screen (or even a normal computer screen), detailing what will be done with the data, the user will most likely just press OK until the service is activated. The users *do have the right* to do this, but it means that the ethics of choice is not correct, since they are not really making a choice. (This is really more a question of "ethics of blame" — the idea, often seen in larger organizations, that a choice is morally correct if the maker of the choice cannot be blamed for it afterwards.) Even if we continue with the assumption that ethics of choice is enough, we need to be very careful in how we present such information to users, so that they want to read it and can understand it.

The directive 95/46/EC also talks about the subject's right to deny permission at any time. This is further elaborated in 2002/58/EC in the case of services where the users' data is continually available to third parties (e.g. the UK GSM child-locator services): the user has to have the right, without charge, at any time, to stop such a service. The prerequisite for stopping the service is, of course, knowing that it is switched on.

How does the switching off work in practice in the GSM locationing case? Is the user *aware* that the service is switched on? We conducted a field study of a presence services last summer, which used a GSM locationing service. At the beginning of the study we asked the participants whether they had already activated the service, and if not we activated it together. The participants invariably answered that they did not have the service switched on, but when we then attempted to activate it we noticed that it *was* switched on — the users just were not aware of it. They had enabled it perhaps a year before for testing, and forgot about it.

The GSM locationing service provides an SMS service for querying whether the service is switched on. This matches the technological capabilities of the current mobile terminals, but fits poorly with human capabilities: if you forgot that the system is on, you won't remember to send an SMS either. What such data collecting systems need is a way of indicating *on the mobile terminal screen* the status of the service, the same way the terminal can indicate new messages. This needs support from the terminal manufacturers. For example the Nokia Series 60 Smartphones which would theoretically have the capability for this, do not allow third-party developers to provide permanent on-screen indicators. Of course scaling such notification systems to multiple notifications and making them understandable is not a trivial user interface design task, but it has to be done. Users are capable of understanding indicators of relatively high technical complexity — just look at somebody trying to find good coverage using the signal indicator on a mobile phone.

Users do not want to keep on making decisions about when to release personal data, what data and to whom. Neither are they willing to make up complex, or even simple, rules about such release. Leysia Palen showed [4] an illustrative example of shared calendaring at Microsoft and Sun (employees of which can be assumed to have fairly similar cultural backgrounds): At Sun the default calendar was set up to reveal the descriptions of calendar events (which can be very personal) and at Microsoft just to show free or busy time. At both companies over 80% of users used the defaults. Here the choice was fairly simple — a single yes or no — understandable and, we can argue, non-dynamic in nature.

There are cases where people have started to make decisions about use of private data. Many know the meaning of the 'no direct marketing, please' tickbox on customer information forms and regularly tick that. It might not impossible to have users make these choices. The choice has to be practical enough (people know what direct marketing is), visible (it's on the same form) and easy to make (just tick the box). Nevertheless, the current reality remains: In most cases where we argue that our systems are morally correct since they allow users to make choices, the argument doesn't quite hold water.

3 Consequences and alternatives frameworks

It seems that the ethic of choice has problems in both practical implementation and matching users' desires. Should we use another ethical framework then? John Artz argued [5] that since computer systems are so complex and pervasive, the application of any consequence-based ethical framework is problematic and we should fall back on virtue ethics instead. In my opinion his arguments are lacking however, and we shouldn't dismiss the importance of consequences even if they *are* hard to predict. We must as system and user interface designers, however, abandon the idea that giving the user choices is enough in the moral sense. We must also weigh the possible consequences, and perhaps try to offer only "safe" choices.

How do we make choices safer, then? The german data protection act actually states that services that act on personal data should be implemented anonymously or pseudonymously, as far as feasible. Many of the proposed location-based services, e.g. location-based proactive information provision, such as special offers to nearby shops, are eminently suitable to anonymization. We could even go as far as making the whole mobile subscription anonymous as much as possible (it is already possible with pre-paid subscriptions).

Most of the discussion here focuses on issues that are applicable to all services that use personal data, including all location-based services. There are, however, two kinds of location-based services with very different characteristics: services where only an organization (or even a system) needs to know the user's location, and services where that location is transmitted to other humans within the social network of the user (e.g. a friend-finder application).

In the organizational case, the issue is much easier. The constraints imposed by the regulatory framework limit the risks to the user immensely, and often people are mostly worried of two things: annoying and distracting communication (like direct marketing), or the feeling of being stalked or watched (in the Orwellian sense). These can be foreseen and measures can be taken to prevent them. Here the ethical issues are perhaps most in taking into account what people actually like (e.g. oppt-in for direct marketing, although this doesn't please the marketing departments) and making organizations accountable for their actions — and the legislation pretty much does this already. (The funny thing being: the directive's focus being on the ethics of choice, in which it maybe fails, it is very effective in actually providing *specific norms* for organizations.)

Transmitting location to other people has to be done much more carefully, and it might prove very difficult indeed to do at all. Recent research into people's willingness to give out their location (in review, so no cite yet) shows the extremely dynamical nature of location disclosure to even very close people. Modelling these dynamics in a computer system does not seem feasible with current technology, so we are left with the need for people to control the disclosure themselves. Here are the truly interesting problems for user interface design.

References

1. The European Commission: Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L 281:31–50 (1995)
2. The European Commission: Directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications). Official Journal of the European Communities L 201:37–47 (2002)
3. Spiekermann, S., Grossklags, J., Berendt, B.: E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM conference on Electronic Commerce, ACM Press (2001) 38–47
4. Palen, L.: Social, individual and technological issues for groupware calendar systems. In: Proceedings of the SIGCHI conference on Human factors in computing systems, ACM Press (1999) 17–24

5. Artz, J.M.: Virtue vs. utility: alternative foundations for computer ethics. In: Proceedings of the conference on Ethics in the computer age, ACM Press (1994) 16–21