

Privacy and freedom of choice

Ana Viseu

The general discourse over technology usage is one of freedom of choice. You chose to adopt or not to adopt a technology, to use or not to use it. This argument allows for only two explanations: One, you choose not to use it because you don't like/want it (e.g., it poses too many risks, takes too much time, etc); or, second, you choose to use it because you like/want it (i.e., you think it is helpful, saves time, etc). In both cases it is assumed that the individual is making a clear and aware choice about the usage and characteristics of a technology.

Within the context of the privacy discussion the "freedom of choice discourse" translates into arguments of the style, "You don't have to give information. No-one's forcing you to use the Internet" [1], into "opt-in/opt-out" policies and into views of privacy as a commodity to be bought and sold.

This "freedom of choice" discourse is deceiving. It assumes at least three things that cannot be taken for granted. First that one is indeed free to choose; second, that one is aware of the dangers; and third, that the context in which one chooses will remain stable over time.

Is there real freedom of choice for users? In the early adoption phase of a technology it can be said that most of its users do, in fact, use it voluntarily. For example, the early internet enthusiasts or email adopters. However, the same cannot be said when a technology has penetrated society's imagination/perception (I believe this penetration does not necessarily have to be "real". See for example, the greed and need of all corporations to have an e-commerce when still almost no one is making money of the web; or the inflated stock values of companies without a business plan). Nowadays, for many the choice of not using the Internet, for example, is fairly limited or non-existent. Even in school children are being "asked" to do their homework using the Internet and to post their work online. Anecdotal evidence comes from the story of a Dutch 64-year-old politician who quit his job because he was unable to cope with the pressure of the amount of email he received each day [2].

The longer the more, you are not given the freedom to choose whether to use, or not, a certain technology: Can you tell your boss that you no longer want to use email because you don't want to be monitored? Or your teacher that you don't want to type your paper because you prefer to write by hand? No. Not really. Making such choices would have disproportionally negative consequences.

Is there freedom of choice if you don't know the ramifications of the options? Even if people were always free to choose, choice presupposes awareness. For, how can I choose if I don't know what I am choosing from? The privacy dangers of using certain technologies or performing certain activities - calling a medical help line, for example - are not always clear. For many of those who are not technology literate, privacy threats are but a hot topic on the press. (I think this explains why many

surveys put privacy as a top concern on peoples' minds but in practice most people don't have any clear strategy to protect their privacy).

Given the current trends of making computing invisible, of making "transparent" interfaces for example, ubiquitous and/or embedded computing knowing who/what is behind certain activities is increasingly hard. As the visibility of the technologies decreases, so does awareness and accountability.

How free is choice if the conditions can change after you have chosen? The sociotechnical environment created by the Internet and other networked technologies is not static. In fact it is so dynamic that most people would agree that we live in a "revolutionary" age. Both the technology and the user change with the time and usage and so do the potential threats. What five years ago was considered common practice, e.g., giving your real name when posting on Usenet, may now turn against you. The expectation that the conditions under which one made a decision will not change is not a rational one.

The expectation that the "usage" of the data that is being collected will also not change is even more irrational. The previous Usenet example also applies here, for now, with new technologies that archive any and all messages posted the medium is altogether different. But this is not an Internet-only issue. For example, an American ice-cream business sold its name-list of consumers claiming free sundaes on their birthdays to a marketing firm. The marketing firm then sold it to the Department of Defence. Soon afterwards all male ice-cream eaters started receiving draft registration warnings on the mail for their birthday [3].

The outcome of discussing privacy in terms of personal choice is that it results in the commodification of privacy itself. It encourages the belief that everyone "owns" his or her right to privacy. It is a given, your given, and you can sell it to others at your own convenience. So, it is argued, can choose to allow my insurance company to "talk" (i.e., have access to data from) my kitchen. In this way, I can be rewarded for having a salad instead of a cigarette; Or, if I drive safely I may want to allow my insurance company access to my car in order to lower my insurance price [4].

You don't have to go into the complicated new technologies that allows access to information that was previously unknown (such as genetics) to see how this is potentially dangerous. There is a fine line between voluntary and compulsory, between freedom of choice and no freedom at all is a very thin one. A look at the current use of invasive job-interviews, where employees-to-be are subjected to a barrage of personal psychological tests and intimate questions. Nobody is forced to release the information, it is voluntary. However it is also unavoidable and vital for a full insertion in the job market, and thus, in society at large.

All this indicates that a privacy discussion framed along the lines of freedom of choice is missing the point (and problem) that freedom is often imaginary or ephemeral. What is needed is a new model for designing privacy into technology. Rather than being designed assuming that individuals will have the freedom of choice to use or avoid them, technologies should be designed with the a priori knowledge that if they are to be successful the individual will have little choice [5].

For privacy advocates this implies shifting from a model based on “choice” (e.g., the fight for opt-in vs. opt-out policies) to one that is more grounded and emphasizes the connection between offline and online practices. It is necessary to re-evaluate the privacy discourse in terms of the real needs (and practices) of those using the technologies. What is needed are not more options, but new default configurations that account for the constraints under which people have to make decisions.

[1]
http://dailynews.yahoo.com/h/zd/20000912/tc/libertarian_candidate_takes_on_silicon_valley_1.html

[2] <http://www.theregister.co.uk/content/6/20231.htm>

[3] Lyon, David. (1994). *The electronic eye: The rise of surveillance society*. Minneapolis, MN: University of Minnesota Press. p.10

[4] Example taken from Gershenfeld, Neil. (1999). *When things start to think*. New York, NY: Henry Holt and Company.

[5] McLuhan once said, albeit in a different context, that “the more freedom there is in the machine, the less freedom there is in the person”.