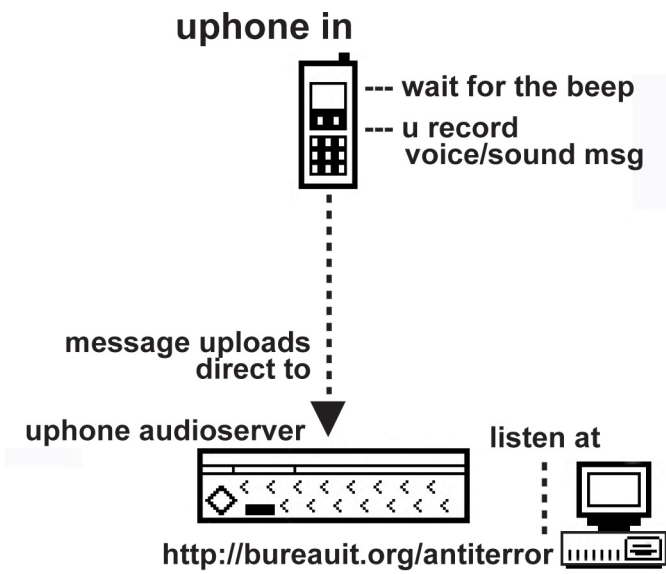


ANTITERROR LINE: ANTI INTELLIGENCE AND THE PATRIOT ACT

project by Bureau of Inverse Technology
text by Natalie Jeremijenko

+



The antiterror line is a project that enables phones – any mobile phone – to be reconfigured as a microphone and which uses this pervasive technology to capture data on an insidious social phenomenon: the infringements on civil liberties in the name of anti-terrorism, made legal in the United States by the Patriot Act and proliferating under Homeland Security measures. The input side to the antiterror line is not unlike most voicemail systems where you can record anything. You can access this voicemail system in the event of an antiterror attack – as you are being escorted off the plane for the national emergency of using the first class bathrooms while the other bathrooms were busy, or had your equipment seized and destroyed because the airport security didn't know what it was, or chased by eight New York State officers and Federal police and taken off a train for wearing rollerblades in Grand Central station (to list a few of my own recent experiences of the transformation of civil society in the name of anti-terrorism). With the phone number preprogrammed into the quick dial of your phone, with one 'Excuse me, I am just turning my phone off', you can discreetly record the events for legal posterity. Your recording will upload in near realtime to the antiterror webpage, the file will be named simply by the time of the recording. (It takes about 5-7 minutes to appear.) Later you can annotate the file and describe the event if you like – the sound quality is probably not great so your elaboration is useful – or someone else who witnessed the event can, or you both can. Even the officer who detained you can annotate. You can, of course, call-up anytime and leave a report. You can identify yourself and other actors or not, you can use it for evidence or not, but in any case, it is there, at least a trace of the event, marked, and accumulated, publicly writeable, publicly readable, and reinterpretable. Most of these 'antiterror' events that compromise civil liberties, are by themselves fairly minor inconveniences, and are not actionable. However, it is the accumulation of these micro-incidents that may provide evidence for a definitive response, or many such responses.

Contrast the antiterror line with former Attorney General John Ashcroft's project for recruiting millions of Americans to report activity they think is suspicious to law enforcement authorities: Operation TIPS (Terrorist Information and

Prevention System). Ashcroft, though not an information technology expert, had to defend the technical design of his so-called 'snitch system', and he did not have an easy time. Ashcroft assured members of the Senate Judiciary Committee on 25 July 2002, that reports of suspicious activity would not be retained in a central database (which, of course, they are). In addressing the concerns surrounding how this information would not be improperly handled and could pose risks, he told the Senate committee, he did not want them to be kept permanently in a central database – but was unable to specify his political ideology in terms of the technical constraints of the database. The Bush administration launched Operation TIPS in ten cities in August 2002 targeting up to one million American workers 'who, in the daily course of their work, are in a unique position to see potentially unusual or suspicious activity in public places', according to the Operation TIPS Website. These TIPS 'volunteers' as they were called on the official site – specifically truck drivers, mail carriers, meter readers, train conductors and other workers – are asked 'to report what they see in public areas and along transportation routes', file the report on the government Website, or by calling a toll-free hot line. As volunteers they are not paid to assume the risks of looking for, finding and acting on suspicions – which in other situations would warrant witness protection measures. Moreover, there is a social cost with respect to the cumulative effect these unknown, unprotected informants can have on the fabric of social cohesion and social trust.

Both Operation TIPS and the antiterror line exploit the distributed presence of many people, and their actual intelligence, judgement and experiences. Although their topic or purpose and their technology may seem similar, they deploy very different structures of participation. They have a financial asymmetry marked in the first three digits. The TIPS line is a toll free 800 number of the type offered by larger entities, business (and only sometimes government agencies) to lower the barriers to participation. Civil society, that is the cultural workers, civic services, quasi-governmental organisations and NGOs, not-for-profits and educational organisations – the sort of organisations that Theda Skocpol argues are the basis of participatory democracy – rarely have the funds to supply an 800 option; as

such, a toll-free number is very useful for marking the power asymmetry that is implied in a financial asymmetry.

Both Operation TIPS and the antiterror line accumulate responses; both have a central database, which was the focus of the judiciary committee's concern; however, this similarity is a red herring. The antiterror line could well be on a distributed platform, like Gnutella, and so could the TIPS line, like say Napster (in combination with some IP blocking, it could work essentially in the same way), but while the difference between these two P2P clients may escape the general public's attention, the structure of participation does not. Condition two, the asymmetrical access to information, does not depend on a central or distributed database, both can be closed, both could be open to scrutiny. With the TIPS line, you are not sure what happens to your input, or even if it was useful. If it was useful, you may be at actual risk, and if you are at risk, what is the protection offered to you? How do you know that the data cannot fall into the wrong hands, now, or years from now, or that your colleague has not found out that you reported that you saw him talking to men who looked 'Arabic', for instance? You simply cannot know since you do not have access to the data.

There is a costly process to filtering information. But the cost of the closed approach amounts to more than the vague unknown risk and discomfort of losing control of one's information: it is the filtering cost that is arguably the most significant. Being able to see other posts helps you assess if a contribution may be useful or not. Lurking, as it is called online, enables people to develop good information filters. The antiterror line exploits both the distributed filtering and distributed judgments of many individuals. Anyone can go to the website and see other contributions, judging if they have anything of value to add, if and how their experience compares, to learn what counts as a civil liberties infringement or to 'get a sense'. Learning if and how to contribute is more difficult to do in the case of closed databases which require explicit instructions. If the capacity to self-filter is reduced, that means the system collects more junk and must bear the cost of excess information, i.e. pay someone, or develop processes or

algorithms to filter all the contributions.

In the TIPS database, workers were asked to be surveillance cameras of sorts, collecting information for a powerful entity, without the consent of those they were collecting information about, without being about to control how information is interpreted, and centralising the costs of doing so. By contrast, with the antiterror line costs are distributed; it costs anyone who uses it 10 pence in the United Kingdom or 25 cents in New York. Both are publicly writeable, but only the antiterror line is publicly readable, which also makes it publicly interpretable, and reusable by many people for many situations. This may amount to nothing; however, the probability of the antiterror files being used for many different things – a documentary radio show, a classroom lecture, a remix into ambient track – is certainly higher than for the evidence collected by the TIPS line. Moreover, the antiterror line cannot be compromised. So the costs associated with 'securing' this information are diminished.

The cumulative effect of an open database is not entirely predictable, but is predictably significant. Although both open and closed databases require participation, I would describe the antiterror line as participatory – specifically, it structures participation to maximise the capacity for many to judge, contribute and interpret the social conditions recorded by the system. Of course people participate in the TIPS, however this design does not draw on the intelligence of all of those participating.

↻