3) On an individual level, you can re-evaluate your use of corporate services in the non-political spheres of your life. If the cops looked over the sum total of your communications traffic, what would they get? How do you feel about contributing to shareholder value by giving these services what they want: your attention as a potential consumer?

4) If you're in an organization, you might want to think about using corporate services in a more considered and strategic way. One way would be to conceptualize your use of corporate services as a kind of guerilla strategy. Radical service providers and internet organizations play the role of safe zones, and corporate services are places that you foray into while maintaining secure bases elsewhere. It's obviously the case that there are hundreds of millions of people using Facebook, Google, or Blogger services, and it doesn't make sense to ignore that. In the same way, lots of people go to the Westfield shopping centre or McDonalds every week; this doesn't mean that Durruti, Makhno, or Marcos would consider them a great place for a strategic base.

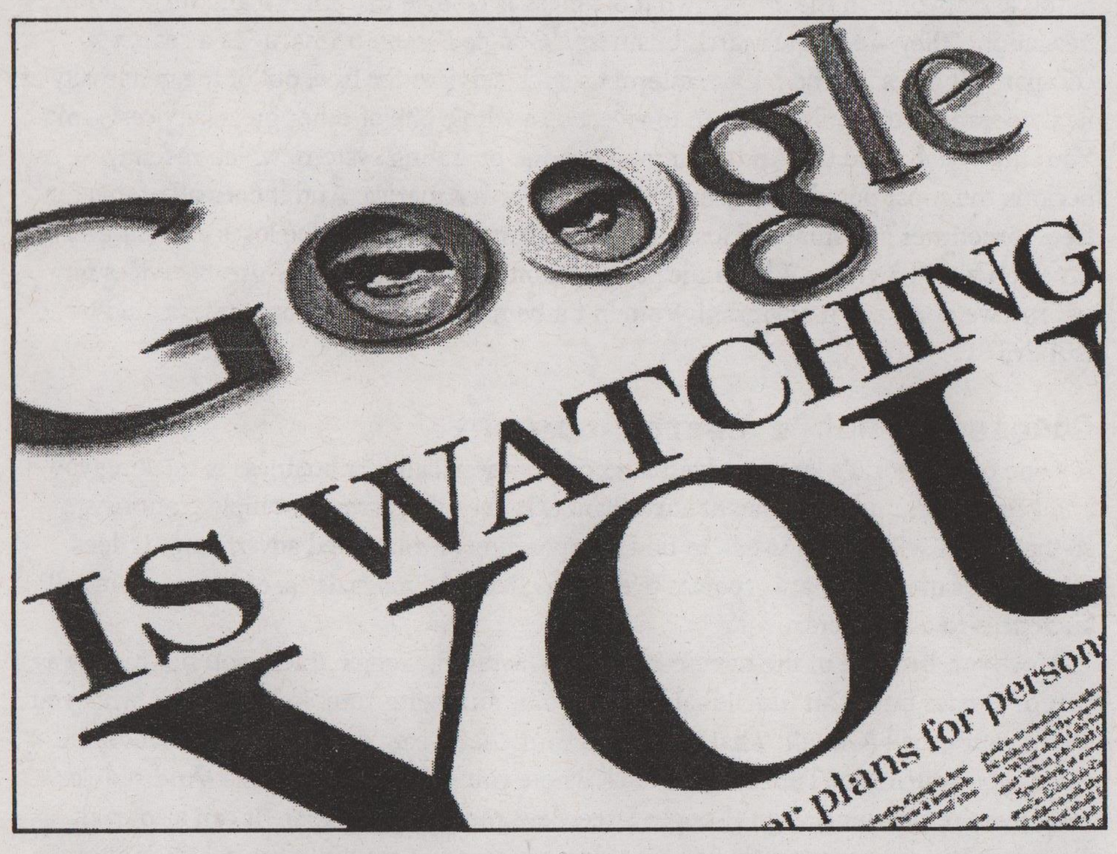
Meanwhile, those of us who write computer code in support of social movements know that we need to do a better job. Ten years ago, we had the upper hand, as the sheer stupidity of the pets.com internet boom put any radical coders who took some initiative way out front of the corporate competition. Today, competing against the development budgets of some very intelligent corporate competition, having no revenue streams, and with our ranks depleted to some extent by both natural attrition and capitalist recruitment, we are at a disadvantage. However, we're still here, and still fighting back in the best way we can: writing secure, privacy-respecting code that enables you to do your work outside the confines of state/corporate surveillance, and without the constant threat of having the rug pulled out from under you.

Since your phone is a computer, and the internet is in the process of turning itself inside out so that it fuses with the street, this job is only going to become more important. We're living in the future, and it's unlikely that you'll get off the internet! But we'll still see you in the streets.

**For further info or to comment:** https://london.indymedia.org.uk/articles/5456








# Their business and ours

If you ask anyone on the street, "what business is Google in?", they'll answer without hesitation, "they are in the search business" but Google is not a search company...

www.london.indymedia.org.uk

If you ask anyone on the street, "what business is Google in?", they'll answer without hesitation, "they are in the search business." Google is seen primarily as a search company. It gives us, the public, internet search services for free, out of the generosity of its corporate heart. It also happen to give a us a whole pile of other great services: Gmail, YouTube, Gtalk, and the Android mobile phone operating system, which recently became the most popular smartphone OS in North America. And it does all of this for free, sometimes at a financial loss - by some estimations, YouTube loses a dollar every time you watch a video. What a nice corporation! It runs all of these great services for us, and we don't pay it anything! Wouldn't it be nice if all global companies could be so Not Evil?

## Google is not a search company.

It's one of the world's largest advertising corporations, and its business is tracking you and keeping you under constant surveillance. It does this across multiple platforms, so that it can sell you, its users, to other corporations for targeted advertising. It does this in the same way that corporate television channels, magazines, or newspapers sell audiences to advertisers.

However, because of the new technologies involved, Google tracks you not merely as part of a mass but as an individual. It does so by analyzing your web searches, what you say in your email (Gmail), what you say in your chat systems (Gtalk), and what online videos you watch (YouTube). It can track where you go with your phone (Android), or where you're planning to go (Google Streetview and Google Maps). It can also track you when you visit apparently non-Google sites, through multiple pay-per-click online advertising networks. And most importantly, it's in a position to tie all of this disparate information together, especially if you log in to Google services with their convenient single sign-on. As a by-product of its corporate mission (generating ad revenue), Google happens to have built the most far-reaching surveillance system in history.

If you ask anyone on the street, "what business is Facebook in?", they'll answer without hesitation, "social networking." However, connecting people with each other, allowing them to share information with each other, and ensuring that they don't miss out on that big party coming up this Friday doesn't make anybody any money. Facebook is in the same business as Google.

## Facebook is not a social networking company.

Although it's been a lot less successful at selling its users to other corporations for advertising purposes, in the past year Facebook has finally managed to become profitable. So it's doing all the same sorts of bad stuff that Google does. The big additional problem for Facebook users, which nobody seems to be talking about, is that although social networking fads are ephemeral, databases are forever. Remember MySpace? Four years after it took the online world by storm, MySpace is in a downward spiral of layoffs, stalled user growth, and upper management turmoil. No one is quite



sure where social networking systems go when they die, but it's a good bet that Rupert Murdoch, who owns MySpace, won't bother worrying too much about the ethics of what happens to all that data. He owns it, after all. His users signed all their rights over to him when they ticked the box and logged in for the first time.

Fast-forward a few years, and Facebook is going to be in the same condition as MySpace, as its users flee the scene to some newer system. In this context, Facebook's "security" model is actually a huge problem for its users, because they don't own or have any effective control over all the data they've generated. Psychologically, because you need to log into it to access all the trash you're talking about people in your "private" messages, it feels safe. If it goes into bankruptcy, or gets sold off to asset-strippers wanting to make a quick buck, what's going to happen to all of the accumulated data? It's not hard to imagine the data being sold and copied multiple times. At some point it's probable that every stupid thing that its users ever said, every human failing or vulnerable moment exposed within its "secure" environment, is going to be on public display.

Regardless of what future problems its users are storing up for themselves, Facebook's business is essentially the same as Google's: advertising revenue generation through individualized mass surveillance.

This surveillance-based business model is not a peculiarity of these two corporations; they're just the most visible. The generation of profit through surveillance is also the main method of capital accumulation behind Yahoo!, Blogger, Digg, every other "free" corporate service, and to a lesser extent Microsoft (which still actually sells some products in addition to being a surveillance company). It's the only reason that business corporations happily lay out massive software development budgets and infrastructure for public use, without charging you for some good or service. They make money, just not directly from their users. They're "free" like commercial television is "free". They're as free as a bunch of advertising executives are willing to let them get.

Putting this amount of surveillance and political decision-making power into the hands of unaccountable private corporations is bad for society in general. Probably the majority of what now passes for "political speech", both public and private, is by now mediated through computer networks and software. Without stopping to think much about it, humanity has given over a huge area of its communal life and self-managed power into the hands of a bunch of capitalist geeks and marketing execs. Looking back, the breathtaking explosion of political speech and action online has been surpassed only by the speed with which it's all been privatized.

This is bad news if you're a political activist, because activists occasionally take actions which are not strictly within the bounds of the law. Unless you're one of the over-privileged few whose main form of political action is getting arrested to "make your point", it's not a great idea to give police access to the details of your illegal activities, either in advance or after they're done. It's not good to willingly give the police any information if you can avoid it. So, it may be interesting to note that one of the busiest

departments in any internet-based corporation is the part of the business that deals with legal requests for information from the police. This aspect of networked businesses has become such a hassle that at least one U.S. corporation has automated the functionality. According to Eben Moglen of the Software Freedom Law Centre:

You have a cell phone and you have a cell phone network provider and if your cell phone network provider is Sprint then we can tell you that several million times last year, somebody who has a law enforcement ID card in his pocket somewhere went to the Sprint website and asked for the realtime location of somebody with a telephone number and was given it. Several million times. Just like that. We know that because Sprint admits that they have a website where anybody with a law enforcement ID can go and find the realtime location of anybody with a Sprint cellphone. We don't know that about ATT and Verizon because they haven't told us.

But that's the only reason we don't know, because they haven't told us. That's a service that you think of as a traditional service - telephony. But the deal that you get with the traditional service called telephony contains a thing you didn't know, like spying. That's not a service to you, but it's a service...and you get it for free with your service contract for telephony. You get for free the service of advertising with your Gmail which means of course there's another service behind which is, untouched by human hands, semantic analysis of your email. I still don't understand why anybody wants that. I still don't understand why anybody uses it but people do, including the very sophisticated and thoughtful people in this room.

And you get free email service and some storage which is worth exactly a penny and a half at the current price of storage and you get spying all the time.

## And for free, too.

Somewhat like self-installed CCTV, this level of surveillance gets individuals busted, but in the case of single-issue "activists", who have no over-arching political goals, that's about as far as the problem goes.

It's worse for anarchists, because if you're an anarchist you at least nominally believe in our ability to act collectively for social change, and in the ability of regular people to organize towards and win a liberatory future. However, all societies have mechanisms to maintain social stability. Any organization which is more than marginally serious about changing the basic political and economic structures of ours quickly runs up against the power of our very own stabilization mechanism: state violence, which needs accurate information to be able to function in an on-target and thus relatively sanitized fashion. Information is what allows the police to pick key people out of the crowd. Metaphorically and literally, it's the difference between surgical attacks on a few people and the indiscriminate beating of thousands, which might provoke a response. It's a crucial component in maintaining social stability - the bad kind.

Alone, we're weak. Like the old song says, "what force on earth can be weaker than the feeble strength of one?". So most of the victories we actually manage to win comes



from our organizations, which we can perhaps characterize as being "fast" or "slow". The "slow" ones are fixed and permanent. The fast ones form quickly, accomplish a set task, and then dissolve, re-forming as necessary along whatever lines of affiliation are tactically convenient. Whatever the relative merits of either mode of operation, it's certainly the case that the internet has been a key enabling factor for both. Which brings us to the main point of this essay.

People routinely do political organizing work using @hotmail.co.uk, @yahoo.com, or @gmail.com email addresses, and corporate "social networking"/surveillance systems are becoming more and more central to the toolbox of the political organizer. But it's not just email or Facebook, and it's not just you - it's all your communications methods, and all of your friends' communication methods. You can be the most secure and righteous individual in the world, but if your friends don't engage in practical solidarity with you by doing the same, all of your communications are going to leak all over the place anyway.

## There are a lot of practical possibilities for police intervention here.

Does one of the people you work with have some financial troubles? Maybe he's doing his sums on Google Docs or talking about it on Hotmail? A quick-fix loan from Special Branch might solve his immediate problems, but at what cost to you?

To get a little steamy, are you heroically breaking out of the bourgeois patriarchal heteronormative monogamy paradigm with the boyfriend/girlfriend/other of one of your comrades when you're not supposed to be? Just once in a while? Maybe talking about it or making dates via your "private" corporate email messages? Nice work, now the cops can know about it too, and if they want to they can make that knowledge public right when it's going to hurt your organization the most.

Planning to converge quickly at a secret location with a few hundred of your friends during a street mobilization and do That Awesome Thing you've got planned? Amazing how the cops seem to always get there first. Perhaps the fact that 99% of us are carrying real-time mobile tracking devices in our pockets has something to do with it. Once everyone is leaking more-accurate GPS data from their shiny new smartphones, the cops won't even need to show up, they can just get us with an airstrike or something, without harming any surrounding civilians. This is an exaggeration, of course, but hardly much of one.

However, it's not just the surveillance aspects of corporate systems that are a problem - there's also a problem of dependency.

For decades, independent media groups have been trying to provide an alternative to the corporate press, precisely because the corporate press has been unable, for institutional reasons, to report honestly or accurately on the politics of anarchist, anti-capitalist, and other anti-systemic political movmements. Despite many failures and problems, in some cases we have been at least momentarily successful in breaking

through the void of corporate coverage and bringing vital social issues into the public consciousness. This happens primarily during spectacular moments of public political mobilization. Though such moments have their obvious downsides, there is a lot to be proud of when we all work together to provide this kind of coverage.

The alternative is the perpetual cycle of radical spokespeople and press groups approaching a corporate reporter or editor, and attempting to ride the wave of an editorial fad for long enough to generate public awareness. This is a necessary activity. But when it's the only strategy, and the radical independent media is treated as merely the poor cousin of the liberal press, there is always the risk of total collapse when the editor decides that the fad is over, or that the political content of a movement has exceeded permissible bounds.

This problem of dependency is magnified when radical groups use corporate services as the basis of their entire communications infrastructure - Blogger for news publishing, Facebook for organization, Hotmail for mail, Google Groups for group discussion.

Building up a for a big political event using Facebook? Don't be surprised if your Facebook group disappears. Police complaints about online organizing are rarely met with a principled response by a corporation whose CEO, Mark Zuckerberg, famously described his users as "dumbfucks" for trusting him with so much of their personal data.

The disappearance of corporate email accounts, Facebook groups, etc. for political reasons already happens routinely. Extrapolating a bit, it's inconceivable that information systems under corporate management are likely to remain stable and functional for anti-systemic activists during any period of major social conflict. The coming year is likely to see an upswing in social antagonisms, with brutal government cutbacks on all of the "nice", redistributive parts of the state and attacks on the living standards of the vast majority of people. The financial crisis must, be paid for by whoever can't defend themselves.

In such a situation, the only anti-systemic political activists who could discount the surveillance capabilities and dependency-inducing characteristics inherent in corporate-controlled information systems are the ones who don't take themselves seriously, who think that they have no hope of ever winning anything, and that they are destined to fail. In other words, "losers". More specifically, people who have decided to be losers. And who wants to work with a bunch of losers? Nobody except other losers.

There are, of course, reasons why most of Britain's anti-systemic movements practise such dismal communications security, make themselves dependent on corporate systems, and regularly do their small bit to boost shareholder value. Computers and communications systems are complex, and most people feel incapable of making informed decisions on technical subjects - so they think, in effect, "Who cares? There's nothing I can do about it."

This is not an altogether unreasonable attitude. The radical geeks who should be the ones to explain the various options to wider social movements often do a very poor job



of providing clear, simple explanations on the subjects that matter. They get bogged down in trivialities, and blurt out incomprehensible techno-speak. Even worse are the hordes of half-competent pseudo-geeks, who invariably have strong opinions and express them loudly despite having only fragmentary or incorrect knowledge of what they're talking about.

The problem is a collective one, and requires a collective commitment to solutions, and a lot of technical work which most groups and individuals don't have the capabilities to address. No one has yet made a clear call to turn the use of corporate systems into a movement-wide political issue, and most people are probably unaware of the magnitude of the problems they are gradually stacking up. The sheer volume of data they are generating about their daily habits, networks of friends and political contacts, and specific plans, would perhaps surprise them if they really stopped to think about it. And they may see no alternative to dependency on corporate systems.

## So, what can be done?

The first, and easiest thing to do, is to talk about the problems with the people you do political work with and decide what (if anything) you want to do. While it's unrealistic to expect that everyone is suddenly going to become a computer-security expert, giving someone in your group or circle of friends the job of doing some basic research tasks will quickly pay off.

If you're that person, here are a few things you might want to consider.

1) There are groups of geeks who are trying to bridge the divide between technical and non-technical people and provide simple, clear, easy to understand advice when it comes to computer use. One example is the Hactionlab, which recently produced a pamphlet called "Tech Tools For Activists: A Non-techies Guide to Tech."

2) There are non-corporate alternatives to corporate services which are run by people you can trust. It's easy to ditch that corporate email address. Every country in the world has its radical internet service providers (aktivix, autistici, mayfirst, nadir, nodo50, riseup, and many more). Most of them offer safe, reliable email services which are not under corporate control. They don't let anybody spy on your communications, they have technical and legal structures in place to defend your privacy and anonymity, and they are doing an immense amount of work to keep their users safe and their systems working during times of heightened repression.

Many of them have proved their courage through their unwillingness to co-operate with the police despite threatened or actual arrest. They are noticed much more often by the police than by the people on whose behalf they collectively do many tens of thousands of hours of technical work each year, mostly without pay. They are rarely thanked, so from one appreciative user: thanks!

If you have any money or time to spare, consider sending them a donation or doing a fundraiser, they need help expanding the scope of their services. Most importantly, they need lots of people using their services, and solidarity when they are attacked.