PRIVACY INTERNATIONAL

Privacy as a Political Right

March 2012

Privacy as a Political Right

Abstract

When we think of privacy in the political system we tend to recall historic events like Watergate, secret files held by governments in war-time, and blacklists. Modern political surveillance is more advanced and sophisticated. In this report we identify some of the modern political surveillance initiatives by governments around the world. We must recognise that all political systems require privacy to function, and devise our policies and build our technologies accordingly.

Introduction

The Wall Street Journal reported recently on the protests in Iran, and referred to YouTube footage of one female protestor who was chanting at the police: "Take my picture, film my face – you can't silence me."[1] I hope that is the case. I hope that is the case. I am doubtful, however. I wish we lived in a world where that was true. But it is likely she will be found, and that there will be repercussions: in January, Iranian authorities warned that they were monitoring emails and text messages to find anyone encouraging protests. In the same week, Google announced that hacking attacks from China were targeting the email accounts of human rights advocates.

These cases reminded me of a recent ominous speech by Stavros Lambrinidis, a Vice President of the European Parliament. He was reminding an audience of international privacy experts of life under the Greek military government. He recalled that the government at the time kept track of everyone's reading habits by monitoring their choices of newspaper. Through this, they were able to know a citizen's political leanings. This was a stark reminder of the chilling effect of surveillance in Europe's political history.

1. 'Iran Protesters Take Broader Aim at Regime', Farnaz Fassihi, Wall Street Journal, December 28, 2009.

These stories remind us of the strong links between censorship and surveillance. A free media is considered an integral component of a new, developing, or established democracy. Free speech is therefore a political right. But today we seem to have forgotten the chilling effect that surveillance plays. Yes, of course, we may point to history to understand this point: the Red Scares, the blacklists and use of informants; the Gestapo techniques; Stalin's spying on friends and competitors and midnight raids; FBI files on politicians and leaders, and Watergate; or the Stasi's network of spies and neighbours. Following from these abuses, safeguards were established to prevent surveillance from corroding our democracies. Privacy was established as a political right. For instance, U.S. constitutional jurisprudence on the right to privacy emerges from the political right to organise and to petition the government and to espouse your beliefs without having to disclose your name, dating back to a case where the State of Alabama compelled the National Association for the Advancement of Colored People (NAACP) to disclose its membership list.[2]

But our minds always go back to those older case studies when we think of the abuses of surveillance powers. When we think of 'democratic safeguards' we rarely think of privacy, but rather we think of fair justice systems, free and fair elections, transparent government, a free media, amongst other components of an open society. Privacy is considered rarely, except for occasional stories of 'Big Brother' government, or as a consumer right. We have forgotten its importance to the protection of democracy. Now that our societies' infrastructure has dramatically changed through the expanded use of technology, our situation is even more precarious.

Privacy in the Political System

As privacy advocates and academics, we spend a lot of time speaking to sceptical audiences. Privacy is perceived as an issue of some import, but hardly on the same level of importance as other political rights. In worse environments, privacy is seen as a mere convenience while the government seeks the powers to do everything it can to defend the country, or the state. As a result, though our talks always include a recitation of privacy's place in all the world's human rights declarations, conventions, and treaties, our audiences often remain unconvinced of its importance.

By November 2008 my colleagues and I were tired of travel and felt accursed, as I found myself speaking to an audience in Bangladesh on 'the right to privacy'. My colleagues and I were in the last stages of an exhausting tour taking us through nine countries in Asia and Eastern Africa. Everywhere we went we faced storms. Some of these storms were real (a Typhoon hit the Philippines on our last day there), some were economic (as the world teetered on economic downturn). The ones that concerned us most were the political storms: some were early-stage (we had to sneak into the Government House in Bangkok as thousands of protestors organised outside), others were erupting (the opposition leader in Malaysia was arrested, again, for sodomy charges, again), and some were violent (our hotel in Pakistan was bombed a couple of weeks after our visit). Our audiences were patient but apart from internet issues, they didn't necessarily understand the importance of privacy.

2. National Association for the Advancement of Colored People v. Alabama, 357 U.S. 449 (1958).

The Bangladeshi audience in November only began paying attention to my talk when I disclosed breaking news to them, of a storm of a British nature: a Member of Parliament had just been arrested by counter-terrorism police for publishing leaked government documents. Officers conducted simultaneous searches of Conservative MP Damian Green's constituency home and office, his office in the House of Commons (without a warrant), and his London home (though they first surrounded the wrong home). His crimes included: gaining access to internal government documents that when published embarrassed the Labour Government on immigration issues; receiving a list of Labour MPs who were likely to rebel against the Government's anti-terrorism plans to detain terror suspects without charge; amongst others. He was fingerprinted, and his DNA was taken. The police went through his old love letters to his wife and his daughter's books, seized his files, computer and Blackberry. They searched through his emails to discover whom he was communicating with, in particular whether he had been speaking with human rights critics of the Government. Centuries of respecting 'Parliamentary Privilege' to protect MPs were swept away, as the Opposition party began sweeping Green's home, offices and car for bugs.[3] Political leaders, critics, luminaries and editors decried how this was 'Stalinesque', or akin to the actions of the Stasi, or 'something that Mugabe would do'.

Every time we repeat this story, and dozens of other recent examples from around the world, the rooms are full of disbelief. Other recent cases include:

- The Bush Administration intercepted conversations of Democrat Congresswoman Jane Harman in 2005, suspecting that she was cooperating with known Israeli spies, as she sought their support to get her appointed as chair of the House Intelligence Committee if the Democrats won the next election. Curiously, the Bush Administration did not proceed on the issue in 2005 as they felt Harman was a valuable ally who could urge the New York Times to not publish a news story uncovering the Bush Administration's telecommunications surveillance programme.[4]
- French magazines gained access to the papers of the former head of the Renseignements Generaux (RG) police intelligence service in 2008. The diaries showed that the RG kept notes on a variety of ministers and critics of former President Jacques Chirac, including their financial information, sexual orientation and habits, and histories of drug use.[5]
- Police in the UK were accused of having contravened the 'Wilson Doctrine' by twice recording conversations of Labour MP Sadiq Khan as he visited a constituent in prison.[6] The 'Wilson Doctrine' was established in the 1960s when the Government, under Harold Wilson, pledged to not tap the phones of MPs. As his conversations were only bugged, not intercepted, it was decided that the Doctrine had remained in tact.

3. 'MP's home swept for 'police bugs'', BBC, December 5, 2008.
4. 'Gonzales Intervened on Lawmaker, Ex-Officials Say', Mark Mazzetti and Neil A. Lewis, The New York Times, April 24, 2009.
5. 'Nicolas Sarkozy affair revealed in notes of ex-spy chief Yves Bertrand', Charles Bremner, The Times, October 10, 2008.
6. 'MP was bugged twice, report says', BBC, February 21, 2008.

These are some of the cases we know of, in countries that have traditions of open government. Put in this light, however we begin to understand that privacy is not some value, or something that can be given away in exchange for security. Privacy is a key defence of a healthy democratic system.

Safeguards are traditionally in place to protect politicians' privacy because there is a feeling that their ability to organise and act is integral to the political system. Collecting secret information on these individuals is a threat to the integrity of the political system. For instance, in 2009 a plot was uncovered in the UK where the Prime Minister's head of strategy and planning devised a plan to smear the leader of Tory Party as suffering from an embarrassing medical condition such as a sexually transmitted disease. The plan was to only allege that the evidence existed, and require the victim to come forward with alternative evidence, thereby disclosing his financial and medical records.[7] Ironically, the UK Government is developing a national database of medical records from which much of this information could be accessed.

Surveillance of Political Movements

Privacy is not a privilege that belongs only to Parliamentarians. The surveillance of political movements, and of individuals' political preferences also threatens political integrity. Just as the U.S. Supreme Court ruled that the NAACP membership lists must be kept secret from the antagonistic government of the State of Alabama, the monitoring of political movements may weaken those movements. Often that is the intention of the surveillance.

- Colombia's intelligence agency, the Department of Administrative Security, over a number of years spied upon the current President's political opponents, critics, human rights workers, journalists, and members of the Supreme Court. One human rights lawyer recounted that in their attempts to find evidence that he was receiving money from the guerillas, the DAS compiled a file on him including his financial information, but also consisting of photos of his children, and transcripts of phone and e-mail conversations. [8]
- Italian Prime Minister Silvio Berlusconi's television channel secretly filmed a judge who had ruled against him in a bribery case. In October 2009, the TV channel aired footage of hidden cameras that followed the judge around, passing commentary on his actions and his choice of socks. This prompted the National Association of Magistrates to file a complaint to the privacy commissioner of Italy, stating that this what an unprecedented attack on a judge, "denigrating a person and delegitimising an essential and delicate function".[9]

7. 'McBride and Draper emails: 'Gents, a few ideas'', Gaby Hinsliff and Mark Tran, Observer, April 12, 2009.
8. 'A Scandal Over Spying Intensifies in Colombia', Simon Romero, New York Times, September 17, 2009.
9. 'Fury as Berlusconi judge filmed', BBC, October 19, 2009.

- The membership list of the far-right British National Party was leaked publicly. The list included the names of over 10,000 members, including members of mainstream political parties,[10] police officers, soldiers, civil servants, teachers, and church ministers. The employment situations of these individuals were placed at risk by the disclosure of the list.
- Russia maintains a court-designated list of terrorist organizations.[11] Legal experts have raised concerns regarding the vague definitions of 'terrorism' and 'extremism' in the law, which permit selective and unpredictable measures against political or media activity critical of the authorities.[12] Human rights campaigners have claimed that the law was being used to spy on human rights groups.
- Reports continue to emerge about the U.S. Government's surveillance practices targeted at political groups who posed no threat to homeland security, including pro- and anti-abortion groups,[13] peace activists,[14] Muslim organisations,[15] and even communities.[16] The U.S. has also chilled charitable giving in the Muslim community under its initiatives to clamp down on terrorist financing.[17]
- There have been a number of initiatives by the police in the UK to monitor protestors, including the use of lists, spotter cards of individuals who may "instigate offences or disorder", and intelligence databases.[18] The police already videotape protests and take photos of participants; with facial recognition technology this practice would be akin to demanding the ID cards of all participants.

10. 'Former Labour, Tory and Lib Dem members on BNP list', James Meikle and Helen Carter, Guardian, November 21, 2008.
11. 'Federal Law no. 35-FZ on Counteraction of Terrorism 2006.
12. Committee of Experts on Terrorism of the Council of Europe, National Legislation of the Russian Federation: Federal Law NO. 35-FZ of 6 March 2006 on Counteraction Against Terrorism, adopted by the State Duma on 26 February 2006 Endorsed by the Federation Council on 1 March 2006.
13. 'Intelligence Improperly Collected on U.S. Citizens', Charlie Savage and Scott Shane, New York Times, December 16, 2009.
14. ACLU uncovers FBI Surveillance of Main Peace Activists, ACLU, October 25, 2006.
15. 'Muslims Say F.B.I. Tactics Sow Anger and Fear', Paul Vitello and Kirk Semple, New York Times, December 18, 2009.
16. 'Loosening of F.B.I. Rules Stirs Privacy Concerns', Charlie Savage, New York Times, October 29, 2009.
17. 'Blocking Faith, Freezing Charity: Chilling Muslim Charitable Giving in the "War on Terrorism Financing", American Civil Liberties Union, June 2009.
18. 'Police forces challenged over files held on law-abiding protesters', Rob Evans and Paul Lewis, October 26, 2009.

Unlike initiatives to arrest individuals, or to censor their speech, a greater problem posed by covert surveillance is that sometimes the groups and individuals themselves do not even know they are subjected to surveillance. This is perhaps the most chilling effect on political organising of them all: you never know you are under surveillance but do not know that you aren't. When the U.S. Congress authorised the National Security Agency's vast telecommunications spying programme, human rights groups and journalists immediately filed suit arguing that the law was unconstitutional as it was likely that their international communications in the conduct of their work would be monitored. This, they said, interfered with their right to free speech and right to be free of unwarranted surveillance. The court ruled in August 2009 that the plaintiffs lacked standing as they could only demonstrate an abstract fear that their communications will be monitored, and that the injury is speculative, particularly as the surveillance would be done surreptitiously. In essence: you have no standing if you can't show you are under secret surveillance, and if you can't show that you've been harmed by secret surveillance, then you have no case.

Modern and Democratic Political Surveillance

All the examples I've given so far are technically similar to the schemes from days of old. The RG case in France isn't much different from the Hoover files in the collection of politically damaging information; the membership list of the BNP isn't technologically much different from the NAACP membership lists. Modern and technologically advanced political surveillance raises the stakes significantly as it first builds the surveillance into the infrastructure of society, and then democratises it in ways that Lambrinides worried about in the Greek Junta where it applies to the general population.

Infrastructure of Surveillance

Modern telecommunications infrastructures are designed with backdoors to enable state surveillance. This began as an initiative of the Clinton Administration when it subsidised and mandated that modern telecommunications devices be designed to assist with law enforcement access. The policy was then expanded upon by the Europeans where 'lawful intercept' was standardised through the European Telecommunications Standard Institute. When we opposed these moves back in the 1990s we were admonished for not believing that democratic safeguards would prevent abuse.

Democratic safeguards and global technology do not necessarily mix well together. The technological capabilities for lawful intercept can be abused. In Greece in 2004, unknown third parties were able to listen to the communications of the Prime Minister of Greece, and dozens of other high-ranking dignitaries over the Vodafone network by gaining access to the lawful intercept capabilities. To this day we are unsure of who initiated the spying.[19]

19. The Athens Affair', Vassilis Prevelakis and Diomidis Spinellis, IEEE Spectrum, July 2007.

More recently these same capabilities were reported to have been used by the Iranian Government to monitor protestors. The Wall Street Journal reported that Nokia Siemens had sold telecommunications technology to the Iranian telecommunications company, and this technology included the 'lawful intercept' standard (though the Wall Street Journal contended that this enabled data interception, Nokia states that it only gave voice intercept capability). This technology is now in place to permit the Iranian government to 'lawfully' intercept the voice communications of opponents to the Government. Nokia responded just as Vodafone did: they were compelled to include these backdoors into the technology by European standards. [20] In light of this, it is perhaps less surprising to hear that the Iranian elite military force, the Islamic Revolutionary Guards Corps, completed a takeover of majority share in the Iranian telecommunications company in October 2009.[21]

Democratising Political Surveillance

With these technological changes, and with the advances in the use of the internet and modern databases, political surveillance no longer needs to be targeted or requires vast amounts of resources. Through a simple subpoena or unwarranted access, vast amounts of personal information on individuals may be accessible by government authorities. Much of this information would have been previously inaccessible to governments. As recent examples,

- In October 2008 the U.S. Department of Justice issued a subpoena to Indymedia's website administator to disclose "all IP traffic to and from indymedia.us".[22] These logs would disclose the identifying information behind all visitors to the website, all journalists and commentators who posted content. Indymedia was also gagged from disclosing the fact that it had received the subpoena.
- In August 2009 Azerbajiani police questioned a number of individuals who had logged a vote using text messaging for an Armenian artists in the Eurovision song contest. Eurovision organisers later stated that they may ban countries from the competition if broadcasters disclose information about voters' identities.[23]
- In Europe, telecommunications companies are now compelled to retain the logs of customers' locations, calls, emails, and other such data for up to two years. Other countries are eagerly following the European lead. In July 2009, the Iranian Government announced new 'cybercrime' laws to protect the privacy of individuals that required internet companies to store all the data sent or received by their customers.[24]

20. 'Provision of Lawful Intercept capability in Iran', Nokia Siemens Networks, June 22, 2009.
21. Elite Guard in Iran Tightens Its Grip With Telecom Move', Michael Slackman, New York Times, October 8, 2009.
22. 'Justice Dept. Asked For News Site's Visitor Lists', Declan McCullgh, CBS News, November 10, 2009.
23. 'Eurovision changes privacy rule', BBC, September 18, 2009.
24. 'Iran to monitor cyberspace to fight offenses', PressTV, July 20, 2009.

Tactics such as these are regularly used to discover the identities of journalists' sources by gaining access to telephone and email logs. The Committee to Protect Journalists 2009 study on the 'Worst Countries to be a Blogger' used a methodology of eight research questions, with three focussing on surveillance.[25]

Social networking services may exacerbate this problem. On these sites, individuals join 'groups' or 'fan pages' and then share this information with large networks. Sexual orientation, political interests, religious faith can be disclosed easily. Even if this information is not willingly disclosed by the individual, two MIT students recently discovered that they could predict an individual's sexual orientation by examining a friends' list.[26] Recent changes to Facebook's privacy settings drew the ire of the Electronic Frontier Foundation who noted that while Facebook celebrates the fact that it is used in Iran, it has now made life easier for the Iranian government to identify supporters of the Opposition.[27] In October 2009 the investment arm of the Central Intelligence Agency invested into a software firm that specialises in monitoring social media, crawling through half a million web 2.0 sites a day.[28]

The Internet is not the sole source of additional personal information for this purpose, however. Vast new datastores have been established in recent years. Governments and companies now run databases that keep information on our financial transactions, medical status, and travel habits; and they share and mine this information on widespread bases. As surveillance again takes place often without the knowledge of the individual under surveillance, there is no way to contest if the Government seeks access to the medical information of critics, or telephone records of Opposition members, critics, or journalists. In countries where Government is the custodian of this information in the first place, unobstructed access to personal information is now possible. In 2008 the UK Government proposed that it become the custodian of all internet traffic data, including social networking interactions; in 2009 the Government pulled back a little and decided to ask telecommunications providers to monitor all internet users and to share this data with the authorities upon request. Meanwhile India copied the 2008 UK plans and recently announced its intention to collect all telephone and email traffic data for the nation.[29]

25. '10 Worst Countries to be a Blogger', CPJ, April 30, 2009.
26. 'Project Gaydar', Carolyn Y. Johnson, The Boston Globe, September 20, 2009.
27. 'Facebook's New Privacy Changes: The Good, The Bad, and The Ugly', Kevin Bankston, Electronic Frontier Foundation, December 9, 2009.
28. 'Exclusive: U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets', Noah Shachtman, Wired, October 19, 2009.' and 'Twitter Tapping', New York Times Editorial, December 12, 2009.
29. 'Centralised System to Monitor Communications', Ministry of Communications & Information Technology, November 26, 2009.

Developing Privacy and Democratic Development

I've always been curious why countries decide to implement censorship technologies on the Internet when instead they can let individuals freely use Facebook, YouTube, access websites of controversial organisations, read articles from banned newspapers; and then they can keep track of everything their citizenry is doing. Informants and covert surveillance is no longer required when we have vast databases, telecommunications companies, and internet service providers who accumulate information on our political interests, hobbies, loves, hates, and fetishes.

We need to renew our safeguards for privacy as a political right. As we sell policies and products to countries around the world we have to acknowledge the risk for abuse; and it is not some abstract risk as surveillance appears in all political systems. My concern is that we are forgetting the political right to privacy as we are indeed spreading our practices around the world. It is thus surprising to me that the audiences in developing countries find our stories about political surveillance so compelling, yet they are often ignored here at home.

All throughout this article I tried to avoid passing judgement on political surveillance. Indeed, some surveillance of political actors is useful for identifying conspiracies, illegal activities, policy contradictions, and hidden interests. The task for regulating these activities is for the media, and the police, with strict controls. When these methods are used politically, and without oversight, problems emerge.

We are forgetting the important role that privacy plays in our political systems, and how political surveillance is corrosive to a democracy. I can foresee two outcomes if we continue to deploy political surveillance without reflecting on the consequences. First, we may face social exclusion as people are more easily identified through their political interests. Discrimination may follow as individuals are identified as members of political groups through their donations, linked to their home addresses, their CVs and social networking profiles. The second outcome is political stagnation. At a simple level this would mean that no one would ever run for office as our private lives as toddlers, children, teenagers, and adults will always haunt our individual political aspirations. More worryingly, those in power will retain their position, enabled through surveillance of their opponents and critics.

We have long built constitutional and human rights into our political systems to prevent abuse by the executive. Free speech is one such safeguard. We cannot forget that privacy is another. This is why democracies have traditionally held secret ballots, protected anonymous petitioners, and created safeguards like the 'Wilson doctrine'. We vowed that we would not let surveillance inhibit political autonomy, development and expression. We must repeat this vow, and it must be updated and enhanced to counter modern political surveillance techniques.

The day may soon come that our whole lives and those of political activists and politicians are recorded in various databases; and someone could easily bring together a mere six megabytes of information about the most honest of us and find enough to hang you or me.