Privacy “And”? Surveillance

Subhajit Basu
Privacy “And”? Surveillance

Subhajit Basu
School of Law
University of Leeds
Email: s.basu@leeds.ac.uk
Surveillance

- Digital Surveillance 'Worse than Orwell'
- Threat Levels as “Unprecedented”
- Government is using the Fear of terrorism to persuade the Public that they should give up their Rights (Open Rights Group)
- "Less and less sympathy with those who oppose” (Boris Johnson on the surveillance debate).
• Mark Zuckerberg, the founder of Facebook, stated in 2010 that privacy is no longer a social norm.

• Privacy understood in terms of "control"

• Lord Neuberger, President of the UK Supreme Court, recently suggested that, “at least in many cases” the right to privacy is “an aspect of freedom of expression"
RIPA regulates the use of and access to surveillance by public bodies.

This involves five types of different surveillance:

- Interception of communications - e.g. listening to telephone calls, reading letters and emails
- Intrusive surveillance - e.g. placing bugs and filming in private places
- Directed surveillance - e.g. filming and covertly monitoring specific people generally in public places
- Use of covert human intelligence sources - e.g. informants and undercover operatives
- Accessing communications data - e.g. accessing the record (but not the content) of emails, telephone calls and websites visited
Does anyone Understand RIPA?

- “We have found RIPA to be a particularly puzzling statute”
  \( R v W \ (Court \ of \ Appeal) \ 2003 \)

- “I do not think the ordinary person or Member of Parliament would be able follow the Act without a lawyer…”
  Sir David Omand Former Director of GCHQ
  (evidence to House Affairs Select Committee) 2014

- “Undemocratic, unnecessary and - in the long run - intolerable”.
  David Anderson QC
• After Paris attacks, UK politicians suggest fast-tracking new surveillance laws

• An undesirable reaction?

• Home secretary Theresa May in a statement made to the House of Commons on the UK's response to the Paris attacks said it is: “important that this landmark legislation undergoes proper Parliamentary scrutiny”
The Investigatory Powers Bill

- The interception and reading of communications - this can only be carried out if approved in person by the Home Secretary.
- "Interference" with computers - including hacking - to acquire information or for some other investigative reason.
- A legal obligation on companies to assist in these officially sanctioned hacking operations.
- The collection of massive amounts of internet or phone data so that it can be later sifted looking for leads and patterns of criminality.
• A new investigatory powers commissioner will oversee the new powers

• Warrants for surveillance will be issued by ministers but only acted on when approved by judges, what is called a "double lock"

• Make provisions for intelligence agencies to acquire information in bulk

• Formalise the Wilson Doctrine, meaning the communications of MPs can't be accessed without approval from the Prime Minister
• Edward Snowden has called the Bill the "most intrusive and least accountable surveillance regime in the West"

• It is "breath-taking" and an "attempt to grab even more intrusive surveillance powers".
UN special Rapporteur on Privacy

- Systematically review government policies and laws on interception of digital communications and collection of personal data.
- Identify actions that intrude on privacy without compelling justification.
- Assist governments in developing best practices to bring global surveillance under the rule of law.
- Further articulate private sector responsibilities to respect human rights.
- Help ensure national procedures and laws are consistent with international human rights obligations.
Geneva convention style law for the internet to safeguard data and combat the threat of massive clandestine digital surveillance.

UN special Rapporteur on Privacy, Joseph Cannataci