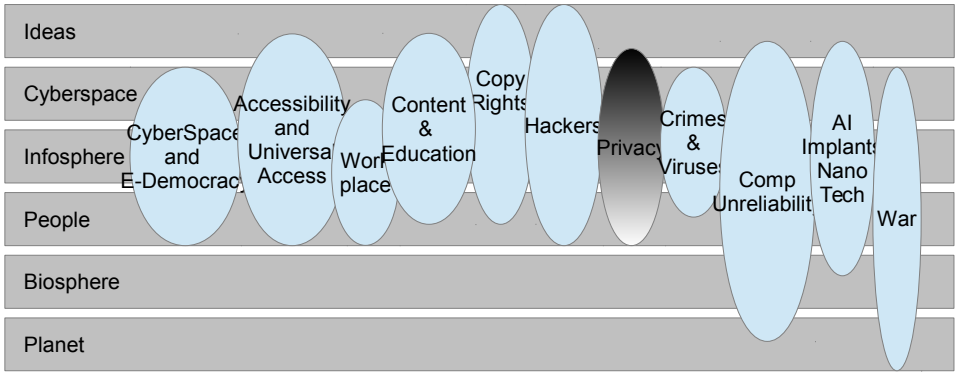
Professional Issues in IT

(~~Spring 2014~~, Spring 2015)

Omar Usman Khan, PostDoc., PhD.
omar.khan@nu.edu.pk

Assistant Professor
Department of Computer Sciences

National University of Computer & Emerging Sciences
Peshawar, Pakistan



Privacy

- Information Privacy = Communication Privacy + Data Privacy
- **Communication Privacy:** Ability to communicate with other people such that the communication is not monitored by other people and organizations
- **Data Privacy:** Limit access of personal data to other people and organizations

Constitution of Pakistan (1973)

- *No one shall be subjected to **arbitrary interference with his privacy, family, home or correspondence**, nor to attacks upon his honor and reputation. Everyone has the right to seek the protection of the law against such interference or attacks. - Article 12*
- *The **dignity of man**, subject to law, the **privacy of home**, shall be inviolable. - Article 14 (1)*

National Cyber Security Act (2014)

- ***Collect or record by electronic means, traffic data in real-time associated with specified electronic documents transmitted by means of electronic devices*** - Article 23 (K) Functions of the Cyber Authority

?? Pakistani NSA ??

13. Immunity of the Council and its Employees, etc.-No suit or other legal proceedings shall lie against the Council or any officer or employee thereof or any person acting under its direction:

(a) for any act done in good faith,-

(i) in the performance, or intended performance, of any function or duty; or

(ii) in the exercise, or intended exercise, of any power, in the capacity of the Council under this Act; or

(b) for any neglect or default in the performance or exercise in good faith of such function, duty or power.

14. **This Act shall be without prejudice to the activities, powers and functions of the Armed Forces or intelligence agencies** or services and shall be without prejudice to the operation of or powers exercised under-

(a) section 54 of the **Pakistan Telecommunication** (Re-organisation Act, 1996);

(b) the **Army Act, 1952;**

(c) the **Air Force Act, 1953;**

(d) the **Navy Ordinance, 1961;**

(e) the **purview of the Intelligence Bureau;** and

(f) **any other intelligence agency or service** that does not itself undertake the investigation or prosecution of any criminal offence

?? Pakistani NSA ??

(4) Any person who by means of an electronic device performs any function, or causes the performance of any function, knowing or having reason to believe that such function will result in **acquisition of a domain name in bad faith to mislead, defame and deprive others from registering the same, shall commit the crime of cyber-squatting.**
... (5) ... shall be punishable with imprisonment of a term not exceeding **three years, or fine not exceeding Rs 500,000/-, or both**

26. Subject to the regulations prescribed by the Cyber Authority, the Investigation Team shall be entitled to:

(a) **access and inspect the operation of any electronic device and any data or program residing therein;**

(b) **access and inspect any information, code, program, technology and other tangible and non-tangible materials;**

(c) **require any person to explain or clarify any matter related to any electronic device whether in his ownership, or control.**

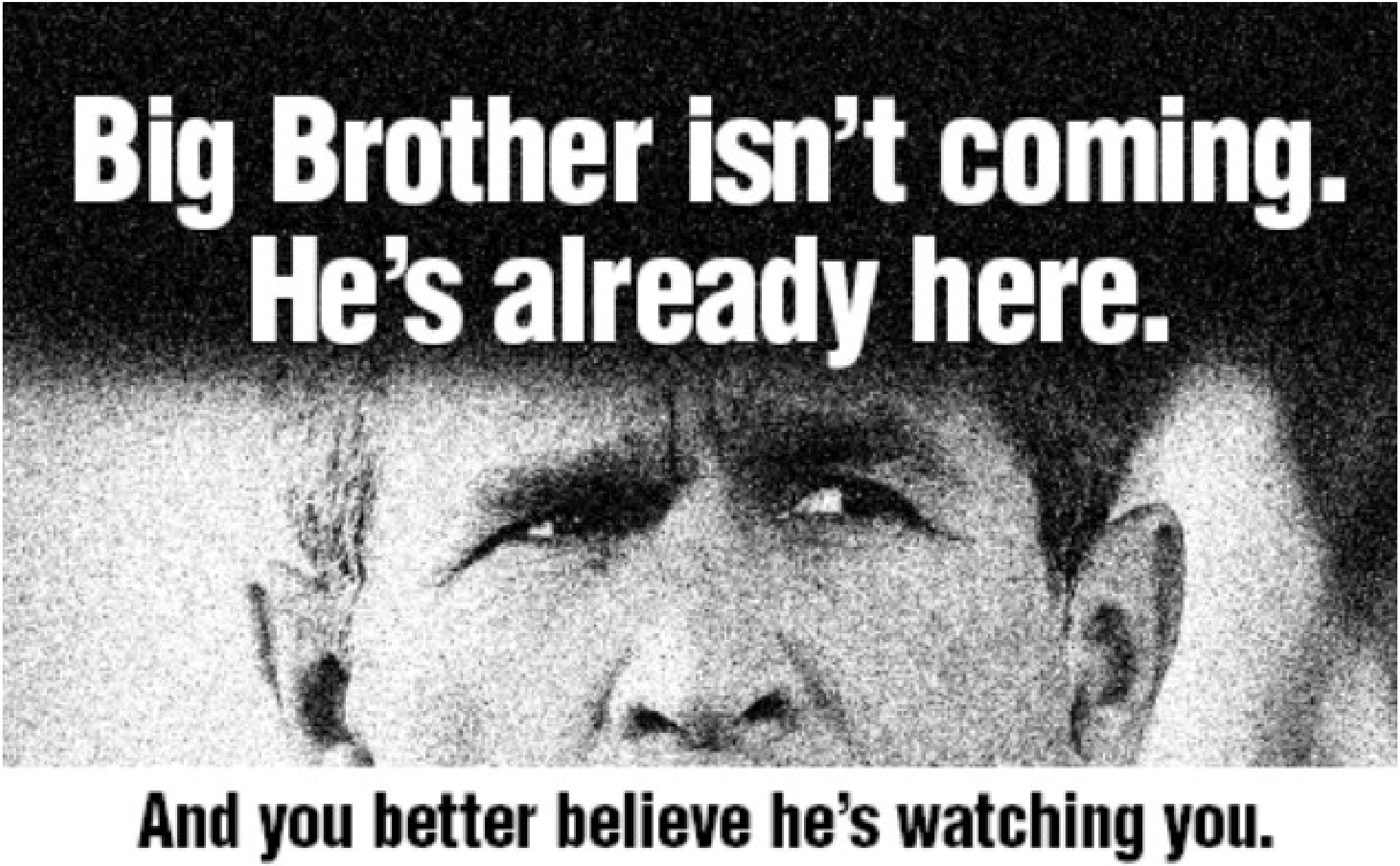
?? Pakistani NSA ??

Scheduled Offenses under **Protection of Pakistan Ordinance (2014)**

- (vi-iii) Killing, Kidnapping, extortion, assault on foreign officials, social workers, officers and armed officers of government of Pakistan, tourists, etc.
- (xii) Destruction of oil pipelines, or liquid and national gas facilities
- (xiv) **Crimes against computers including cyber crimes, internet offenses and any other offense related to information technology.**

Burden of Proof: Accused facing the charges of scheduled offense on existence of reasonable evidence against him, **shall be presumed to be engaged in waging war against Pakistan unless he establishes his non-involvement in the offence.**

Punishment: Scheduled Offense shall be punishable with imprisonment which may extend to 10 years, with fine, confiscation of property, unless the scheduled offense already provides a higher punishment.


Big Brother isn't coming.
He's already here.
And you better believe he's watching you.

- Reports directly to the White House
- Budget = 6x CIA Budget
- Computing Power: Strongest, Fastest, and most sophisticated
- Potential of controlling/Listening 70% communication in the world
- 16 December 2005, New York Times,
  “Bush Lets US Spy on Callers without Court (warrants)”
- 10 May 2006, USA Today,
  “NSA has massive database of Americans' Phone calls”

- Edward Snowden (Ex-CIA, Ex-NSA Employee)
- Leaked “thousands” of classified documents described as most significant leak in US History by White House.
- Also leaked dozens of big data tools that the NSA and related agencies used to collect telephone/internet data from the entire world.
- Sparked ethical debate on “balance” between “National Security” and “privacy rights” guaranteed by the american constitution.
- NSA on the back-foot after European telephone tapping controversy

Criticism of Cyber Security Laws

- Criticism
  - Some national institutions/organizations are given more power, which if exercised will directly conflict with the privacy clauses guaranteed in constitution.
  - There is too much ambiguity in interpretation of some laws/articles.
- After-effects:
  - Pakistan amongst the first few in Islamic world to draft laws on cyber security. Good achievement.
  - Rest of muslim countries highly likely to copy Pakistan's laws and apply in own countries.
  - Result = 1 Billion people are at risk of their privacy rights being compromised.

Privacy Issues

- Financial Data:
  - Credit card information, loans, stocks, bank account details, etc.
  - Online/networked access will use information like logon name, password, account number, pin number, advanced captcha's, (and in some countries, finger-print readers)
- Health Information
  - Centralized health system may mean that patient data will be linked/transferred to health facilities around the country. Individuals would be concerned about violation of health related private information going to employers, schools, insurance companies, marketing companies, etc.
- Children's Personal Data
  - As internet use by children continues to rise, they need protection from inappropriate material, online predators. They may be harassed or be cheated into divulging personal information.
  - Note: It is illegal in the USA to get children to sign-up forms without parental consent. Therefore, age limit applied on many services, gmail, facebook, etc.
- Access to government records
  - Pakistan Right to Information Act (2013)
  - Defines process to apply for information held by the government, (information which is otherwise not available to general public)

Privacy Issue: Identity Theft

- When a person steals personal information of another person in order to "impersonate" that person.
- Information may include:
  - Name, Address, Date of Birth, ID Card Number, Passport Number, Driver License Number, Mother's Maiden Name, Name of Pet, Name of Schools, etc.
- With this information, identity thief may:
  - Apply for credit cards, take-up rent at an apartment, setup phone/utility services, do phone & Internet banking, etc. all in the name of the other person.
- How Identity thief gets data:
  - Breaching very very large databases (millions of records)
  - Purchasing identity information from black market
  - Phishing: Tricking users to enter personal information on counterfeit websites.
  - Spyware: Install keystroke-logging software on target without his/her knowledge.

Privacy Issue: Identity Theft: Recommendations

- When disposing of used electronic devices, completely and irrevocably destroy digital identity data on used equipment (Emphasis: Destroy … not Delete)
- When disposing of information on hard-paper, shred everything before dumping to garbage.
- Write "Request Photo ID" on back of your cards so retailers may ask for it every time.
- Ensure nobody is peeking/looking at you from your behind your shoulder, when you are giving personal information out. (e.g., filling forms, or at the ATM).
- Do not write your identification information on documents such as receipts/cheques, etc.
- Do not use Debit Card for Purchases. Use Credit Cards. Credit Card owners have no little/no liability if their card gets mis-used. Debit Card owners can have their entire balance wiped out.
- Dispose of credit card receipts carefully (shred them)
- Use hard to guess passwords and bank pin numbers.
- Don't share your personal accounts with others.

Privacy Issue: Consumer Profiling

- Companies build profile of consumers when they register @ websites, complete surveys, fill online-forms, enter online contests, etc.
- Companies also obtain user profile information by installing "cookies" on client machines, or by installing tracking software in form of "toolbars".
- Websites also come with "click tracking" scripts.
  - E.g., Google Adsense can allow you to determine which region of your web-page generates the most number of clicks.
  - The clicks also model the flow of clicks from one page to another. So you can build a profile of the most popular paths that your users take.
  - In the end, you are better poised to place advertisements at a right place on your site.
- Why do companies do this?
  - They want to know who their customers are, where they are from, what they like, how they behave, what motivates them to buy.
  - They use this data to tailor their services to you individually, or tailor to your geographic region, or to your income bracket, or to your profession, etc.
  - Increase Sales basically !!! at stake of your privacy.