Adopted resolutions against big data analytics misuse in work practices

Science, Computer Science

The resolutions the one would adopt in his future work practice or the measures to lower the privacy risks:

- Use web browsers which has a “ private browsing mode” that doesn’t save the web history on your own computer, to prevent others from accessing your computer to learn about your browsing
- Use an anonymous browser, like Hotspot Shield or Tor (The Onion Router) when visiting sites that might produce erroneous information about you that could result in drawing inaccurate conclusions by others. When internet users go online, it provides them with anonymity, and obscures where they’re accessing the Internet from, even when they log into sites or use their real name
- Use HTTPS Everywhere, which is a browser add-on that attempts to secure the connection to websites whenever the web site you’re visiting supports it
- Access an email account over a secure HTTPS connection to prevent your ISP, as well as people on your wifi network, from reading your mail as it travels between you and your mail provider.
- However, using email encryption software like PGP prevents even your webmail provider itself from reading the mail
- Use “ host-proof hosting”, which is a service that encrypts data on your own computer before being uploaded to a cloud service. Then the service provider itself can’t read the data you’re storing there without knowing your encryption password. These applications are called “ host-proof” because they provide protection even against the service provider itself

- If you don’t read the entire policy of terms and conditions, you should take a moment before clicking ‘ OK’ to consider why and with whom they’re sharing their information
- Reduce the amount of sharing on social media. If you only have a few people you want to see photos or videos, then send directly to them instead of posting where many can access them
- Don’t provide information to businesses or other organizations that are not necessary for the purposes for which you’re doing business with them. Unless they really need your address and phone number, don’t give it to them
- Ask others not to share information online about you without your knowledge. The hard truth is that users need to protect themselves because nobody else will be doing it for them

Understanding the implications of big data surveillance is more complex than simply knowing who is surveilled more or less. Instead, we need to understand who is surveilled by whom, in what way, and for what purpose. In the last decade, big data has come a very long way and overcoming these challenges is going to be one of the major goals of Big data analytics industry in the coming years.