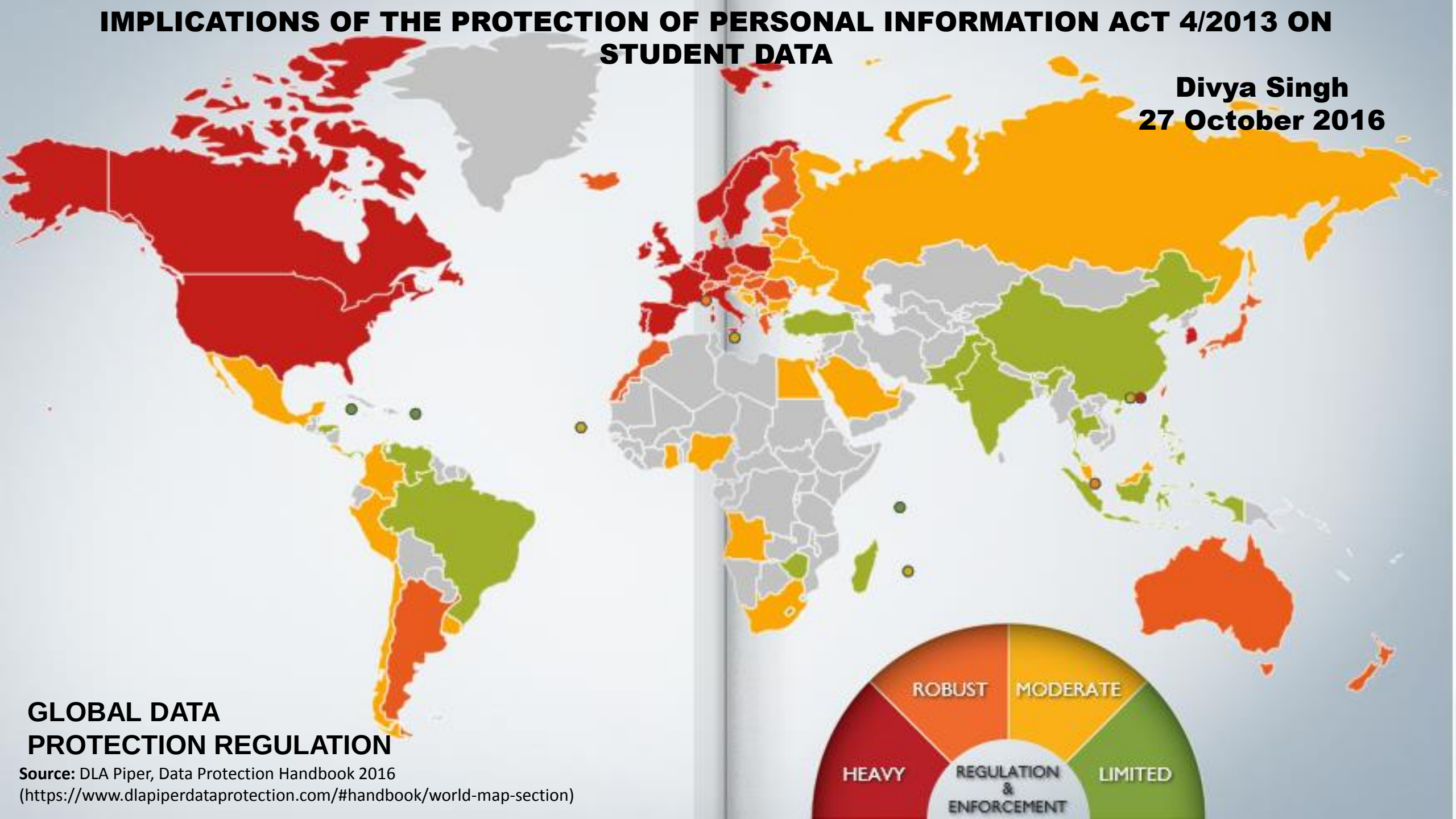
IMPLICATIONS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4/2013 ON STUDENT DATA

Divya Singh
27 October 2016



GLOBAL DATA PROTECTION REGULATION

Source: DLA Piper, Data Protection Handbook 2016
(https://www.dlapiperdataprotection.com/#handbook/world-map-section)

WHAT IS PERSONAL DATA?

Information relating to an identifiable, living natural person (and identifiable, existing juristic person)

- race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, birth
- education, medical, financial, criminal, employment history
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier,
- biometric information
- personal opinions, views, preferences
- correspondence sent by the person which is implicitly or explicitly of a private or confidential nature
- views, opinions of another person about the individual

"That's our CIO. He's encrypted for security purposes."

PURPOSE OF POPI SECTION 2

To promote the protection of personal information processed by public and private bodies and to introduce appropriate conditions which establish minimum requirements for the processing of personal information.

"We have to be forthright with the public. We have to have their confidence. We have to convince them we're working for the common good. *Then* we can invade their privacy."

POPI AND PRIVACY

Protection of Personal Information

=

Data Protection

≠

Privacy Protection

KING III
CHAPTER 8, PRINCIPLE 6

- The Board should ensure that “information assets” are managed effectively.
  - All personal information (which is an “information asset”) must be identified and treated as an important business asset
  - There must be appropriate systems in place for:
    - ✓ the management of information AND
    - ✓ ensuring the security and privacy of information.

DATA COLLECTED MUST BE NECESSARY

- Collection of personal data must be lawful, necessary, relevant and minimal
- POPI, Section 13(1): information must be collected for a specified, explicit, and legitimate purpose
- Canada: uses the test of reasonableness
- New South Wales: is the information clearly appropriate and relevant to the functions of the organization
- Greenleaf: limit the amount of data collected

"Stop staring at my wife!"

NOTICE
IT'S ABOUT 'TRANSPARENCY'

- PRIVACY COMMISSIONER OF CANADA

People should be told what information is being collected about them, by whom, for what purposes: they should be told what is being done with it and who it is being disclosed to; they should be able to control the collection, use and disclosure of the information through the power of granting or withholding consent; the information should be securely held … people have a right of access to their information, and a right to correct it where necessary

CONSENT

- Where personal information is intended to be shared with third parties, the data subject's consent to the USE and SHARING must be obtained
- 'Opt in' versus 'Opt out' options
- Personal information should be collected from the data subject …

SECURITY BREACH

- **Brighton and Sussex University Hospitals NHS Foundation Trust (UK)**
  - Failed to identify a data processor that would provide 'sufficient guarantees' in respect of security
  - Did not contract to force data processor to act on instructions of data controller
  - Failed to conduct a reasonable risk assessment
  - Sensitivity of information is a crucial consideration

- **POPI**
  - There is a clear responsibility on the data controller to ensure that data is 'adequately protected'
  - 'Adequacy' specifically includes *inter alia* a data protection clause in contracts where data is shared
  - Data subjects must be informed that their information is being shared
  - The data subject's consent must be obtained that the information may be shared

SECURITY BREACH

- POPI makes it a mandatory obligation to report and inform affected data subjects in the event of a breach – 'daylight as disinfectant'
- California/Canada/Australia: 'serious harm' or 'serious risk'
  - California - seriousness is an external determination
  - Canada/Australia – seriousness is internally determined
- POPI: 'reasonable grounds to believe that data has been accessed or acquired'
- Assessment of controls:
  - Were there controls in place?
  - Were they appropriate?
  - How strong were they?
  - Apply 'generally accepted information security practices and procedures'

"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

RIGHT TO ACCESS PERSONAL INFORMATION

- Data controller must respond to any request by the data subject to:
  - Inspect data held about them
  - Correct data
  - Remove data
- Where data is stored in the cloud, the obligation remains with the data controller

"It was much nicer before people started storing all their personal information in the cloud."

CONCLUSION

Rather than being viewed as an additional burden to administrative operations and therefore as incurring concomitant costs, data protection laws and the ideals enshrined in them should be embraced for their 'enrichment of our normative space'.

BYGRAVE