Balancing Cyber Security, Digital Rights and Privacy

“***Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet***.”

Justice Brandeis US Supreme Court **1928 (**1890?)

Is there actually anything net new here?

- Asymmetry bargaining power> digital rights
- Network effects > individual choice
- Attack Vectors > software + hardware growth
- AI/ML/Computational speed/Social speed > legal speed
- IoT, Cloud > Individual data control
- Quantum> PKI
- Education/best practices > digital legal protections
- Suggest not Search > Net neutrality
- Content Creation > Freedom of the Press

Tort of Seclusion *Ontario Court of Appeal 2012*

One who intentionally [or recklessly] intrudes, physically or otherwise,

upon the seclusion of another or his [or her] private affairs or concerns,

is subject to liability to the other for invasion of his privacy,

if the invasion would be highly offensive to

a reasonable person.

UC DAVIS LAW REVIEW

VOL. 49, NO. 4

APRIL 2016

Information Fiduciaries and the First Amendment

*Jack M. Balkin**

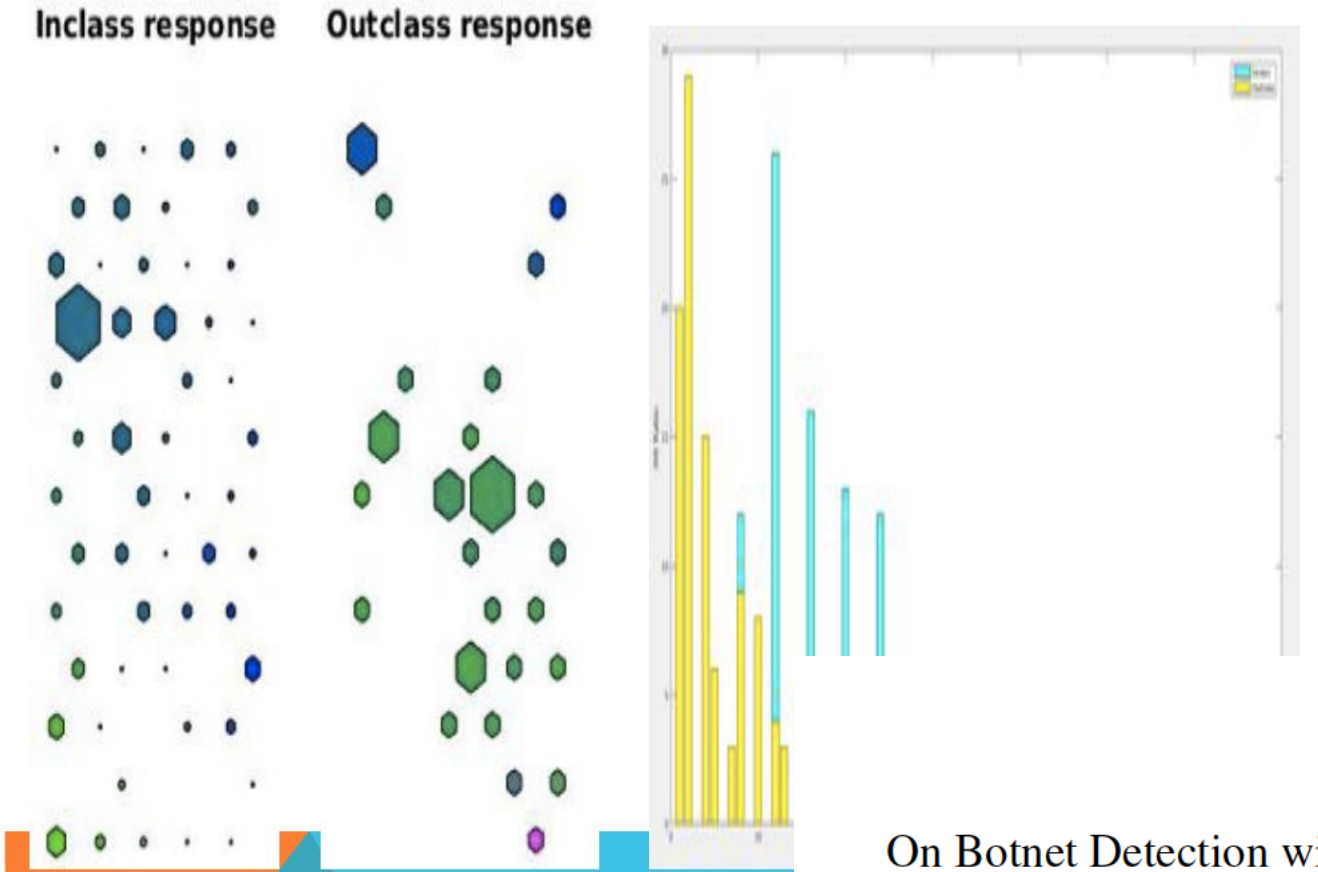
Information Fiduciary

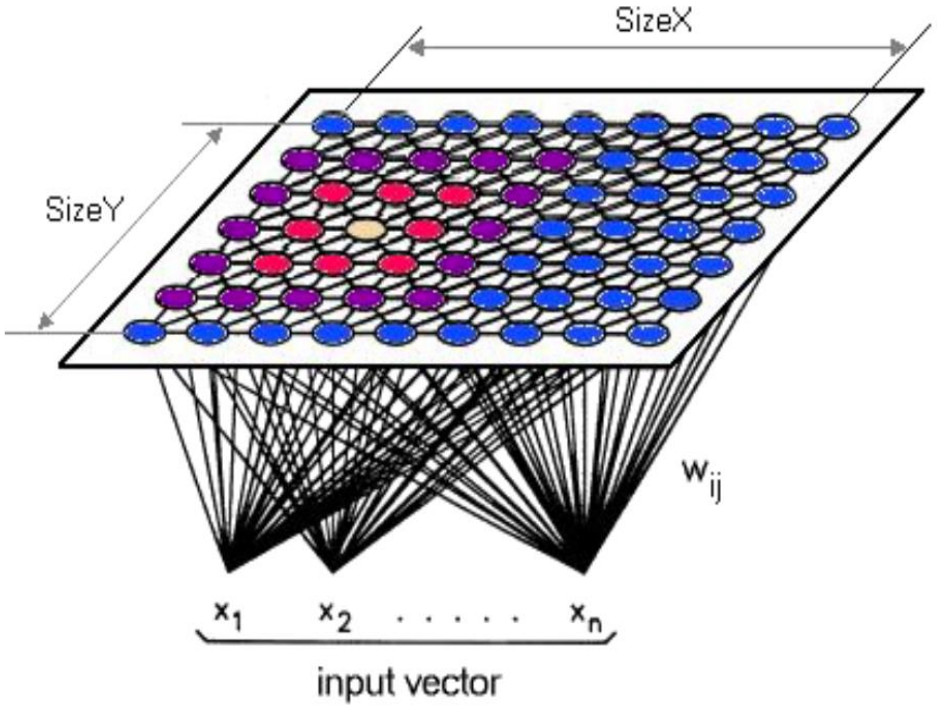
- A *fiduciary* is a person or business with *an obligation* to act in a trustworthy manner in the interest of another.

- An *information fiduciary* is a person or business that deals not in money but in information.

- An information fiduciary must agree to a set of fair information practices, including security and privacy guarantees, and disclosure of breaches.

SOM MODELLING OF USER BEHAVIOUR





"Smart Phone User Behaviour Characterization base
Organizing Maps", D Rajashekar, AN Zincir-Heywood,
International Conference on Data Mining Workshop c
Security, 2016

On Botnet Detection with Genetic Programming Under Streaming Data Label Budgets and Class Imbalance

Sara Khanchi, Ali Vahdat, Malcolm I. Heywood and A. Nur Zincir-Heywood

Faculty of Computer Science, Dalhousie University, 6050 University Av., Halifax, NS. Canada

Balancing the Commons

- Privacy By Design™
- Security by Design (e.g. ITSG 33, 800-50)
- Data anonymization/zero knowledge
- Sample legislation response – European Union
- Right to be Forgotten, GDPR, Explicit Consent
- Government/Citizen combined Oversight
- Humans interacting with computers and data
- AI/ML interacting with Humans? Ethical oversight?

Bill C-59

Fed Treasury Board *draft* policy on AI systems

- People should always be governed – and perceive to be governed – by people;
- AI systems deployed on behalf of government should be trained to reflect the Values and Ethics of the Public Sector as well as Canadian and international human rights obligations; they should be used to reinforce these values where possible;
- Organizations are accountable for the actions of AI systems, and should build systems that are auditable;
- Understanding the need to protect privacy and national security, AI systems should be deployed in the most transparent manner possible;
- Organizations should ensure that reliable contingencies are in place for when AI systems fail, or to provide services to those unable to access these systems;
- AI systems should be developed in a diverse team that includes individuals capable of assessing the ethical and socioeconomic implications of the system;
- AI systems should be deployed in a manner that minimizes negative impact to employees where possible, and should, where feasible, be created alongside the employees that will work with them.


A NEW WAY FORWARD
Beatty St

Thank you