Privacy with Surgical Robotics: Challenges in Applying Contextual Privacy Theory

Shishir Nagaraja and Ryan Shah

University of Strathclyde

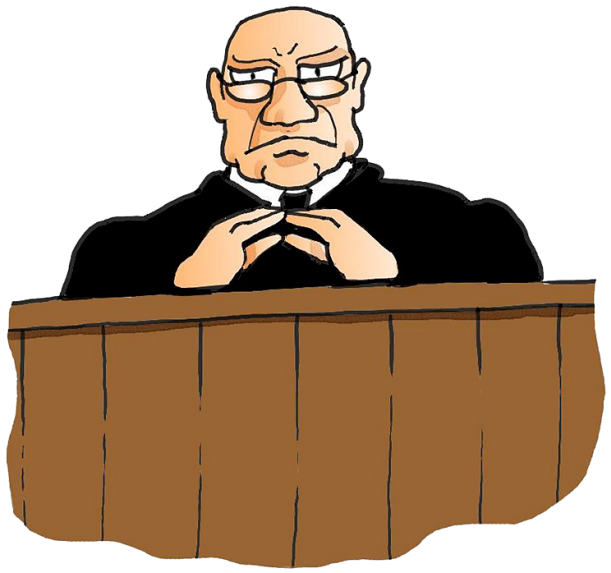
Surgical Robotics

Surgical robots provide:
- High accuracy
- High precision
- Increased efficiency

They can carry out variety of procedures:
- Bone milling
- Controlling blood loss
- Incisions
- Suturing

Patient Privacy

Patient Consent



Regulatory Consent

Observer Consent

Patient Privacy

These protocols are based on patient's faith in:

- Surgeon
- Medical staff
- Hospital standards and regulations
- Legal guardians (and other observers)

What's the threat model?

How do existing mechanisms of privacy control perform, if surgical robots were to replace human surgeons?

In comparison with human surgeons:

-The untrusted party is the robot's software

-So what sort of privacy frameworks can we use to understand privacy leakages.

Existing frameworks are data centric

How do existing mechanisms of privacy control perform, if surgical robots were to replace human surgeons?

Data centric means that privacy concerns are focused on data flows – i.e collection, dissemination and use of personal data.

Existing frameworks are data centric

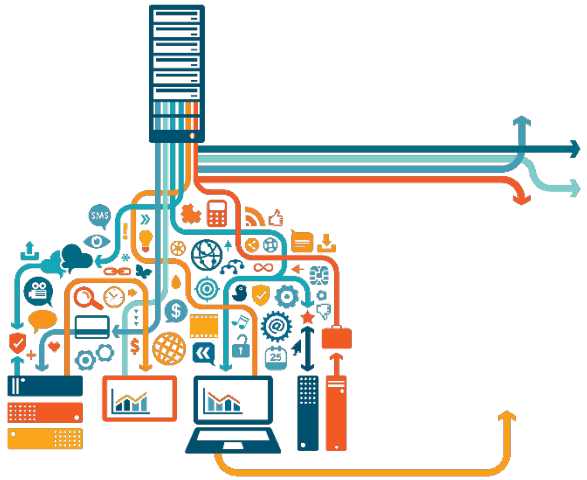
Traditional confidentiality- and privacy-preserving mechanisms and frameworks to manage dataflows were developed when the granularity of control was at the **level of files or information-flows**

Observation

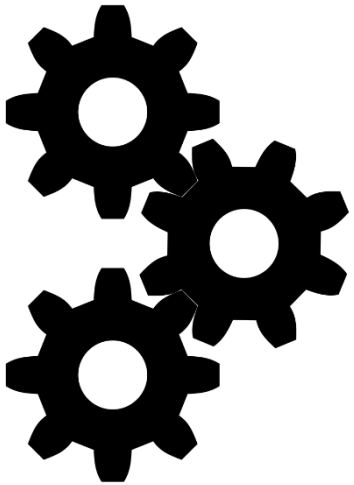
The granularity of control at the level of information flows isn't enough!

So what are the basic `units` or `level' at which control should be exercised?

We propose **four types** of basic units



Data



Services

Subject

Operations

Contextual Privacy and Surgical Robots

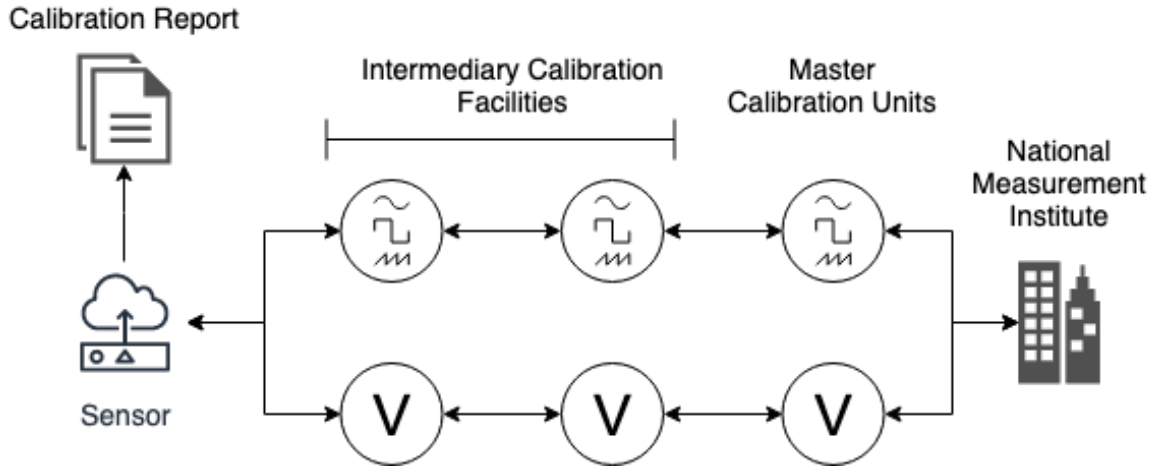
Can contextual privacy theory provide a means for solving this problem?

Replace existing consent protocols with context-based privacy policies

- Fits well with the threat model
- Helps to place patient wellbeing at centre of connected medical environment

Contextual Privacy and Surgical Robots

Privacy is provided by appropriate information flows



Robots must be calibrated to retain high accuracy and precision

- Calibration information flows from a high-integrity source to a low-integrity destination
- Combining calibration traffic and patient information could compromise patient privacy
  - Forbid lower levels writing to higher levels and higher levels from reading downwards

Applying Contextual Privacy

Context	Sender & Receiver	Transmission Principle	Example Norm
On-the-fly calibration	Calibration facilities and the surgeon	Information flows from top calibration level to hospital. Invalid calibration is informed at one-hop stages	During a procedure, the robot must retain valid calibration. If the calibration is deemed invalid, then it must be recalibrated on-the-fly

Points for discussion

Challenge

How can we apply contextual privacy to policies, whilst expressing them in a non-technical manner?

How can we express privacy policies to:

- Rigorously convey risks and outcomes to be enforceable in verifiable manner
- Be conveyed in a manner that is not too technical for patients to understand
- Formulate appropriate norms for surgical contexts

Points for discussion

Is defining policies, for even simple robot movements, too complex for a patient to understand?

A role for expert review on these policies is required

- Conducting formal analysis to mitigate the complexity of policies might help
- Solution should involve experts to govern new forms of privacy controls in connected hospital environments
- Privacy considerations do not apply only to information but also physical “property”.

Questions/Discussion

Main challenge was to express and enforce policies rigorously in a verifiable yet simple manner [verifiable, understandable]

How does one go about dealing with the cyber-physical element, using a consent framework designed for constraining information flows. Is there a way to extend CI to address this?

University of Strathclyde Glasgow

Thank you

Shishir Nagaraja – shishir.nagaraja@strath.ac.uk

Ryan Shah – ryan.shah@strath.ac.uk