HOW SMART DEVICES BALANCE PRIVACY AND SHAPE MIS IN THE COVID-19 ERA – CONSIDERATIONS FOR THE ACCOUNTING & HEALTHCARE PROFESSIONS

SARAH HINCHLIFFE, PHD

50TH WCARS, RUTGERS

NOVEMBER 7, 2020

WHAT THIS PAPER IS AND WHAT IT IS NOT?

- **Review paper** and analysis of the **enabling technologies** as a way to move forward and to deal with the **unique setting of the IoT** with a focus on the interaction between **humans and machines** in the **COVID-19 environment** and its impact on the **Accounting Profession**.

LITERATURE REVIEW – THE IOT

- In an IoT context, there has been a plethora of research on privacy preserving analytics and the like…

Research Contributions	Privacy	Trust for IoT	Security				Identity Management	Data Management	IoT Monetization
			Access Control	Data Integrity	Confidentiality	Availability			
FairAccess [101][102]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zhang et al. [100]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Enigma [103][110]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Shafagh et al. [104]	✓	✓	✓	✓	✓	✓	✓	✓	×
PISCES [105]	✓	✓	✓	✓	✓	✓	✓	✓	×
PlaTIBART [106]	✓	✓	×	×	✓	✓	✓	×	×
Ayoade et al. [107]	✓	✓	×	×	✓	✓	✓	✓	×
Cha et al. [87]	✓	×	×	×	✓	✓	×	×	×
Hawk [33]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Conoscenti et al. [108]	✓	✓	×	✓	✓	✓	✓	✓	×
Sharma et al. [109]	✓	✓	✓	×	✓	✓	✓	✓	×
Rahulamathavan et al. [111]	✓	✓	×	✓	✓	✓	✓	✓	×
JointCloud [112]	✓	×	×	×	✓	✓	✓	✓	×
Hardjono et al. [113]	✓	✓	✓	×	✓	✓	✓	✓	×
Dorri et al. [86]	✓	✓	✓	✓	✓	✓	✓	✓	×
Ali et al. [114]	✓	✓	✓	✓	✓	✓	✓	✓	×
Aitzhan et al. [80]	✓	✓	×	✓	✓	✓	✓	×	✓
Laszka et al. [81]	✓	✓	×	✓	✓	✓	✓	×	✓
Knirsch et al. [82]	✓	✓	×	✓	✓	✓	✓	×	✓
Lombardi et al. [115]	✓	✓	×	✓	✓	✓	✓	×	✓
Gao et al. [118]	✓	×	✓	✓	✓	✓	✓	✓	×
Kang et al. [117]	✓	✓	✓	✓	✓	✓	✓	✓	×
Kang et al. [84], [83]	✓	✓	✓	✓	✓	✓	✓	×	✓
Wang et al. [116]	✓	×	✓	×	✓	✓	✓	×	×
Liu et al. [128]	×	✓	×	✓	✓	✓	✓	×	×
Urien et al. [129]	×	✓	×	×	✓	✓	✓	×	×

LITERATURE REVIEW – THE IOT

- Little research about the interaction between these factors (at a 'foundation level'), notwithstanding that the future MIS is deployed not only in a more decentralized fashion, but also at the machine level.

Bahga et. al [130]	×	✓	×	✓	✓	✓	✓	×	×
Boudguiga et al. [131]	×	✓	×	✓	✓	✓	✓	×	×
DiPietro et al. [132]	×	✓	×	✓	✓	✓	✓	×	×
IoTChain [133]	×	✓	×	✓	✓	✓	✓	✓	×
Psaras et al. [134]	×	✓	×	✓	✓	✓	✓	×	×
Trustchain [135]	×	✓	×	✓	✓	✓	✓	×	×
Tian et al. [136]	×	✓	×	✓	✓	✓	✓	✓	×
Bocek et al. [137]	×	✓	×	✓	✓	✓	✓	✓	×
Samaniego et al. [138][167]	×	✓	×	×	✓	✓	✓	×	✓
Axon et al. [151]	×	✓	✓	✓	✓	✓	✓	×	×
Hashemi et al. [152]	×	✓	✓	✓	✓	✓	✓	✓	×
Novo et al. [153]	×	✓	✓	✓	✓	✓	✓	✓	×
Capchain [154]	×	✓	✓	✓	✓	✓	✓	✓	×
Hamza et al. [155]	×	✓	✓	✓	✓	✓	✓	✓	×
Biswas et al. [156]	×	✓	✓	✓	✓	✓	✓	✓	×
Yang et al. [157]	×	✓	×	✓	✓	✓	✓	×	×
Lee et al. [158]	×	✓	×	✓	✓	✓	✓	✓	×
Steger et al. [159]	✓	✓	✓	✓	✓	✓	✓	✓	×
Alphand et al. [160]	×	✓	×	✓	✓	✓	✓	✓	×
Chakraborty et al. [161]	×	✓	×	✓	✓	✓	×	✓	×
Imbault et al. [165]	×	✓	×	✓	✓	✓	✓	×	×
Kikitamara et al. [166]	×	✓	×	✓	✓	✓	✓	×	×
Kravitz et al. [168]	×	×	×	×	✓	✓	✓	×	×
Huh et al. [169]	×	✓	×	✓	✓	✓	✓	×	×
Lee et al. [170]	×	✓	×	✓	✓	✓	✓	×	×
Liang et al. [189]	✓	✓	✓	✓	✓	✓	×	✓	×
Azaria et al. [190]	✓	✓	✓	✓	✓	✓	✓	✓	×
Xu et al. [191]	×	✓	×	✓	×	✓	✓	✓	✓
Missier et al. [192]	×	×	×	✓	✓	✓	×	✓	✓
Nehai et al. [215]	×	✓	×	✓	×	✓	✓	×	✓
Münsing et al. [216]	×	✓	×	✓	✓	✓	✓	×	✓
Spectre [220]	×	×	×	✓	×	✓	✓	✓	×
Lewenberg et al. [218]	×	×	×	✓	×	✓	✓	✓	×
IOTA Tangle [221]	×	×	×	✓	×	✓	✓	✓	✓
Byteball [222]	×	×	×	✓	×	✓	✓	✓	×
Yu et al. [224]	×	✓	✓	✓	✓	✓	✓	✓	×

MOTIVATION

- Continued growth and reliance on the IoT
  - E.g. The IoT healthcare market is projected to grow from USD 41.22 Billion in 2017 to USD 265 Billion by 2024, mainly driven by growing investments in healthcare market by governments and various other stakeholders.
- Acceleratory effect of COVID-19?
  - presents technical, societal and legal challenges.

MOTIVATION (CONT'D)

- What does this mean for the Accounting Profession and the Healthcare Industry?
  - COVID-19 has spurred the rapid emergence of the IoT;
    - i.e. (i) IoT-enabled devices (e.g. smart devices); and (ii) virtual setting.
  - Greater impetus and ongoing need for an understanding of the evolution of Information Systems – in particular with regards to:
    - **Strategic advice** → Role of management in organizations and the impact on strategic advisory roles;
    - **Who is the 'manager'** → The role of MIS in organizations that are 'using' the IoT;
    - **Regulatory and institutional frameworks** → e.g. self-regulating, jurisdictional-specific or model treaties?
- This is the basis of the model referred to in this study.

CONTRIBUTION

- This study makes **three key contributions**.
  - First, this study contribute to the IS theory-building literature by developing a theoretical framework in the context of the IoT.
    - Framework combines standard arguments from information economics with privacy and liability aspects from legal theory to offer novel insights into the interaction of senders and receivers of information.
    - Importantly, the model shows that **when privacy and liability concerns are classified as costs**, the **value of information disclosure** can be reduced.
  - Second, the author contributes to the literature on decision making by managers and its impact on the strategic advisory role (accounting profession) and healthcare.
    - Specifically, this study highlights that AI machines are expected to assume decision-making tasks previously reserved exclusively to human managers.
    - Similar to human managers, the author argues that AI machines will require MIS to solve decision tasks.
  - Third, this paper contributes to the MIS design literature by moving the “new” MIS to the periphery.
    - In particular, the author shows how the placement at the AI machine-level can mitigate privacy and potential liability concerns of organizations operating within the domain of the IoT and how such MIS can serve both humans and AI machines.

THE IOT IN CONTEXT: INFORMATION DISCLOSURE AND STAKEHOLDER RELATIONSHIPS

- In addition to aiding human planning and decision-making, it also raises major concerns about social issues including privacy, security, and liability issues precipitated by the use of the data.

Table 1. Information Disclosure for various Sender and Receiver Groups				
Type	H2H	H2M	M2H	M2M
Sender	human	human	machine	machine
Receiver	human	machine	human	machine
Granularity	low	medium	medium	high
Information Type	asymmetric	asymmetric or symmetric	asymmetric or symmetric	symmetric
Intelligence	natural	natural & artificial	natural & artificial	artificial
Privacy Concerns	high	high	medium	low
Liability	high	high	low	low

- Table 1 shows that it is especially when a sender/receiver group includes a human that IoT issues cross into the realm of privacy and liability. Increasingly, data that are being collected through these interactions are being analyzed using new “big data” analytic software (Chen, Chiang and Storey 2012).

COMPLEX SYSTEMS AND DESIGNING THE 'NEW' *MIS* ECOSYSTEM

- Complex systems can sometimes be highly connected, enabling the sharing of information and the distribution of power.
  - In political decision-making environments, such phenomena can allow more people at lower levels of society to participate in the policy making process.
- Is this the same for the IoT? Blockchain? Smart device deployment?

- In a public policy and regulatory context, complex systems have several positive attributes.
  - Their connectivity and self-organizing characteristics that facilitate information sharing can help improve situational awareness and problem solving (Lier 2013).
  - Through emergence and coevolution, complex systems can also foster innovation by bringing together information and ideas and creating unexpected positive outputs (Homer-Dixon 2010).
- On the negative side, complex systems can disseminate false information and can result in leadership overload with too much unfiltered information complicating the policy making process.
  - This can lead to policy ambiguity, feeding public uncertainty and anxiety about the future.

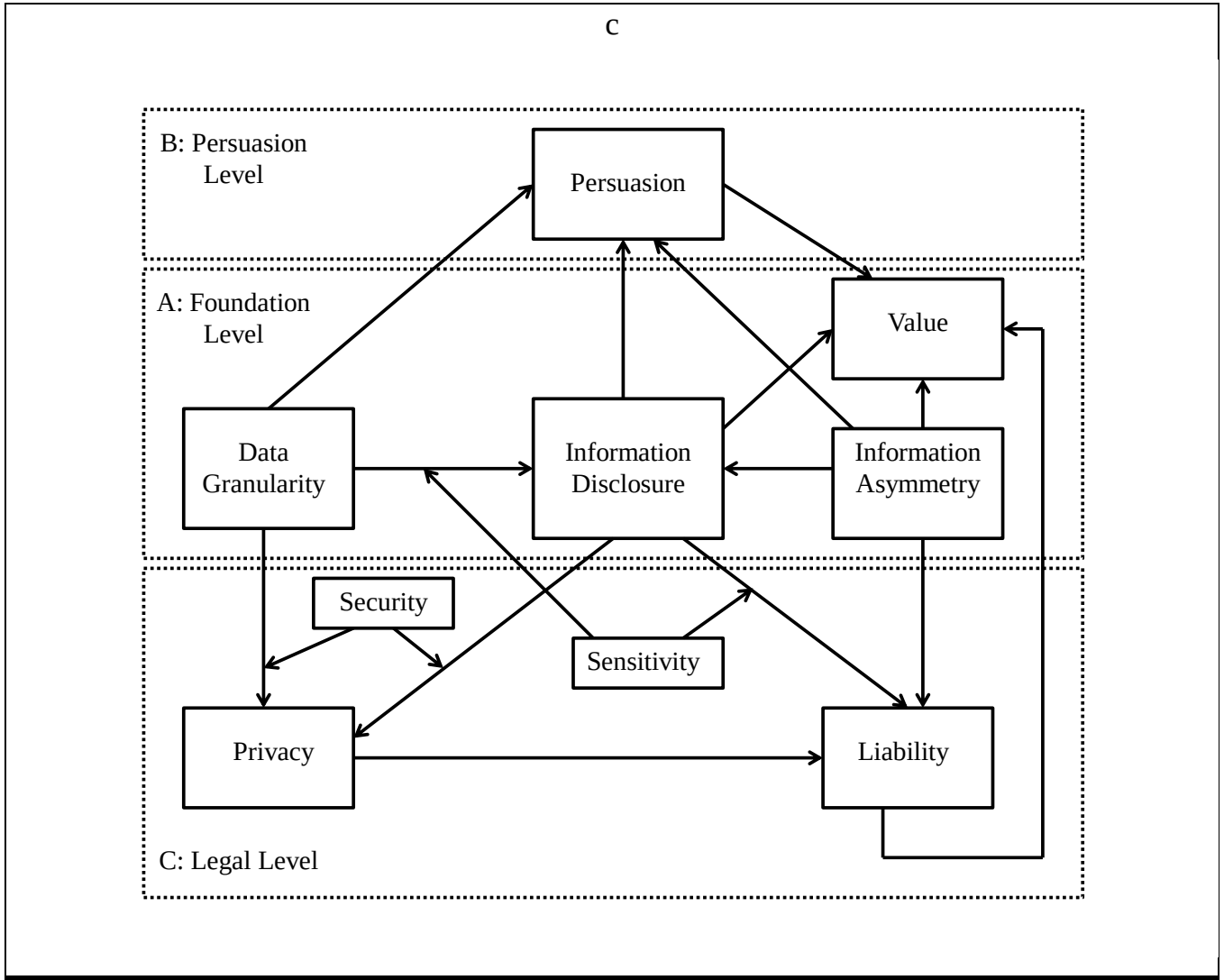
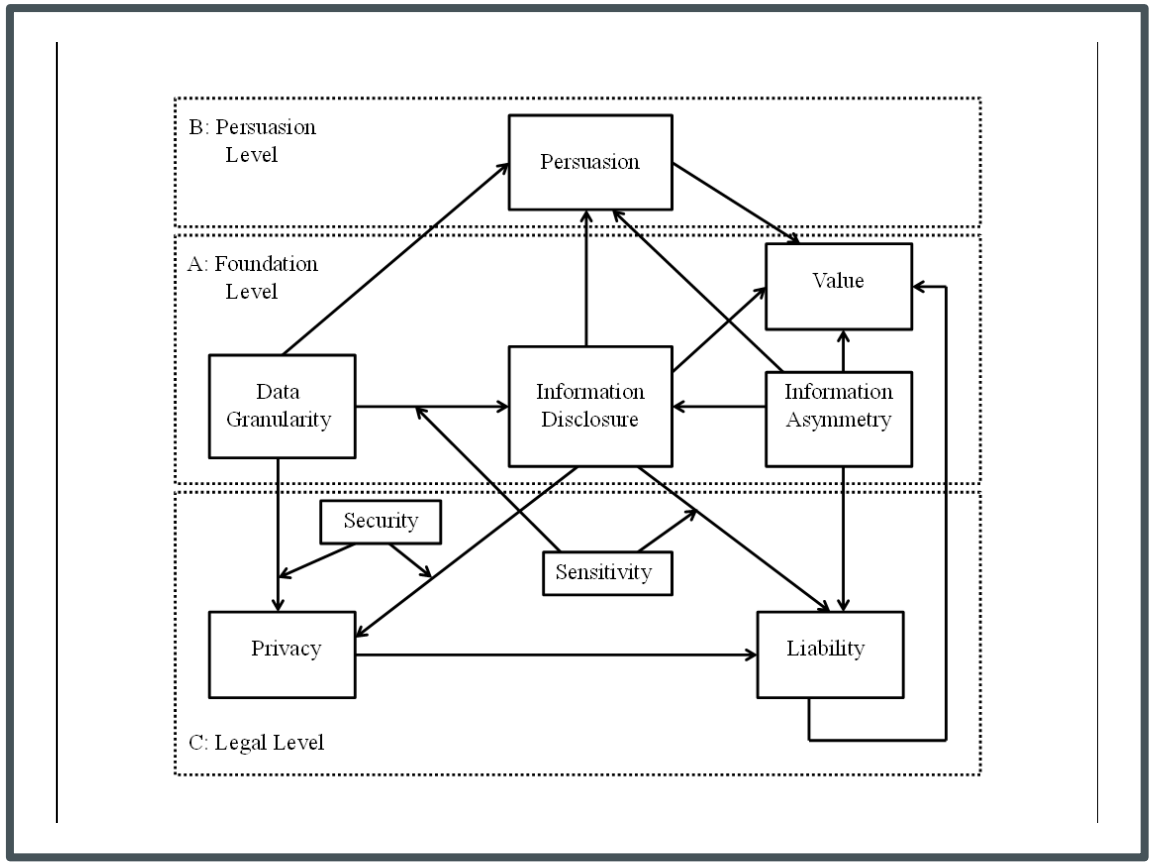


Figure 1. Theoretical Framework of Information Disclosure

THEORY

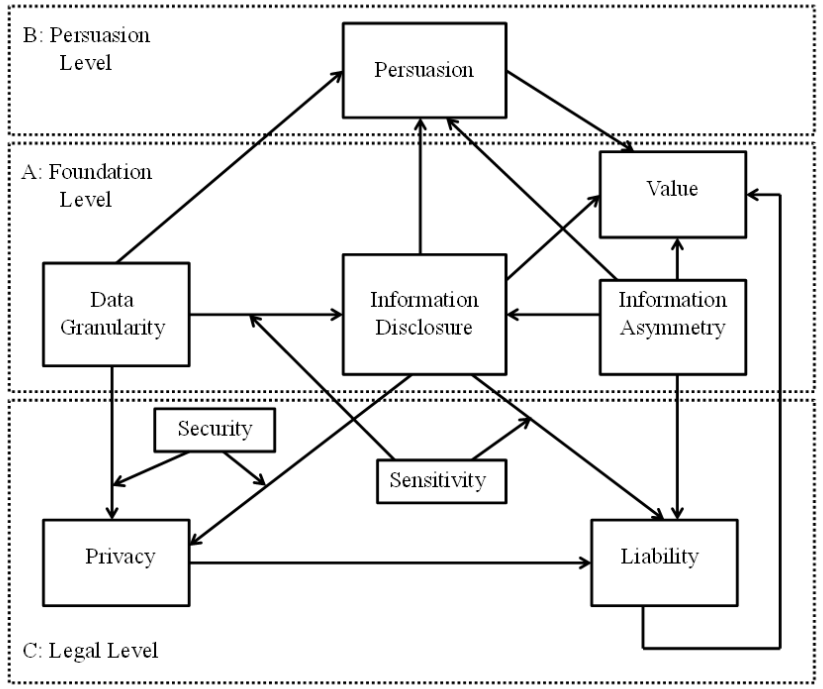
- The design of a new MIS requires a better understanding of the interaction of technological systems and social systems (Lee 2001). The theoretical model is presented in Figure 1.
- The theoretical framework is prescriptive, and as such, it is a special predictive case (Gregor 2006).
- It consists of three building blocks: (1) the foundations of information disclosure; (2) persuasion and information disclosure; (3) and legal aspects of information disclosure.

FOUNDATIONS OF INFORMATION DISCLOSURE



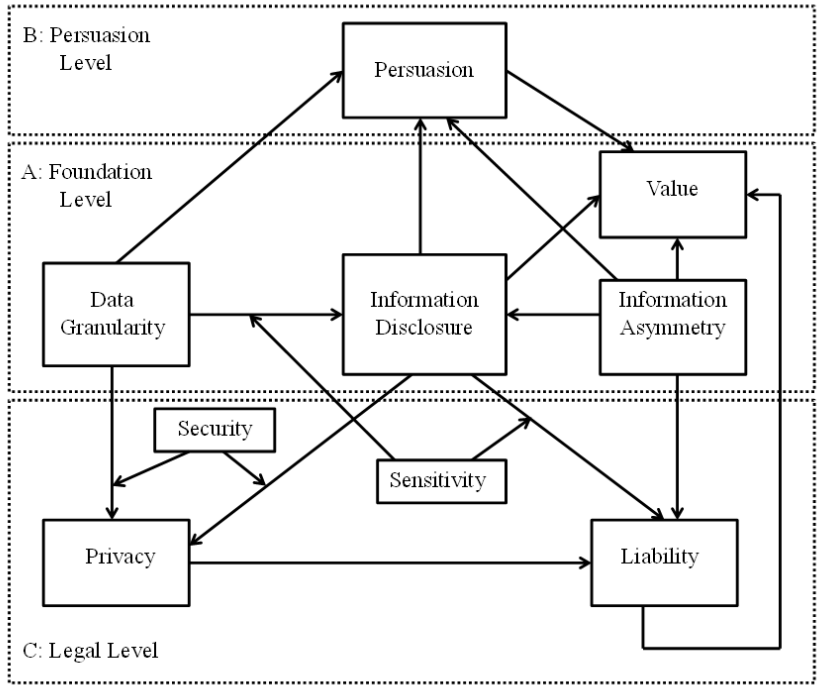
- At the center of this study's model rests information disclosure (see Figure 1, region A).
- In the IoT, data are collected via sensors or devices operated by humans.
- **Information disclosure can occur in two ways:**
  - **(1) as raw data or**
  - **(2) as processed data that have been transformed into information.**
- This information is organized and structured and helps the manager in the decision making process.
- In this study's model, greater information asymmetry between the sender and the receiver reduces value. The sender can deliberately send a wrong signal, which reduces the value of the information for the receiver.

PERSUASION AND INFORMATION DISCLOSURE



- The sender can overwhelm the receiver by disclosing too much information.
  - Although this information is more valuable than less information, it might be difficult to find the relevant information to effectively solve a problem.
- One way to possibly overcome this issue is by persuasion (see Figure 1, region B) (Rayo and Segal 2010).
  - Until now, this strand of research has only investigated situations where there is symmetric information between sender and receiver.
  - Under certain conditions, a sender can persuade a receiver in a fashion that solely benefits the sender (Kamenica and Gentzkow 2011).
  - Interestingly, this work also shows that full information disclosure is optimal in some situations, whereas no disclosure is optimal in other situations.
- In the context of the IoT, interactions between machines, i.e., M2M, are likely symmetric, as machines cannot be dishonest per se.
- Interactions involving humans are likely asymmetric. At the heart of persuasion lies the idea of selective information disclosure.

LEGAL ASPECTS OF INFORMATION DISCLOSURE



- Collecting data with a finer granularity is a costly exercise and, thus, has to be subtracted as a cost from the value of such information.
  - Note that this paper does not specify who ultimately benefits from the value of such information.
- The reason for this is that **who shares in the value is context dependent.**
  - Often, this is the receiver, but it is also possible that the sender or a third-party will benefit from the disclosure of information.
- Similarly, privacy will indirectly affect the value of disclosed information, whereas liability will directly affect it (see Figure 1, region C).
  - Both can be interpreted as a cost and, as such, will reduce the benefit of information disclosure.
  - **Privacy concerns** are mitigated by the level of sensitivity of the information disclosed.
  - The accidental release of less-sensitive information is unproblematic. However, the unintended disclosure of sensitive information can result in serious liability exposure.

LEGAL ISSUES

Privacy Risks and the IoT

- Two key issues at the core of the privacy debate include the following: 1) the desire of an individual to conceal or keep secret private information and 2) the use of private information after it is collected (Weber 2009; Weber 2010). As will be explained, this (the misuse – either accidental or intentional) is closely connected with liability issues.

Security Risks and the IoT

- This problem stems from a disconnect related to security and privacy between electronic and mechanical engineers who design the machines or devices, on the one hand, and the communication engineers who connect and integrate those devices to the IoT, on the other hand.
  - The more sensitive the information transmitted through the IoT, the more problematic it becomes.
- To address this problem, more critical processing can be done at the AI level to only send the relevant information that can be in a desensitized format.
  - The key objective is that the right message be sent to the receiver while simultaneously utilizing the function of AI machines to undertake a large part of the process.

- **Global security standards** and government regulation (similar to privacy?); or **security-by-design (SbD)** (i.e. where manufacturers are required to build prescribed security features into their IoT devices).
- **Do we have a decentralized MIS** (many little MIS interacting) → **use of smart contracts and blockchain**; or do we give more intelligent machines a greater role or responsibility than less important machines?

GRANULARITY, SECURITY, PRIVACY AND LIABILITY

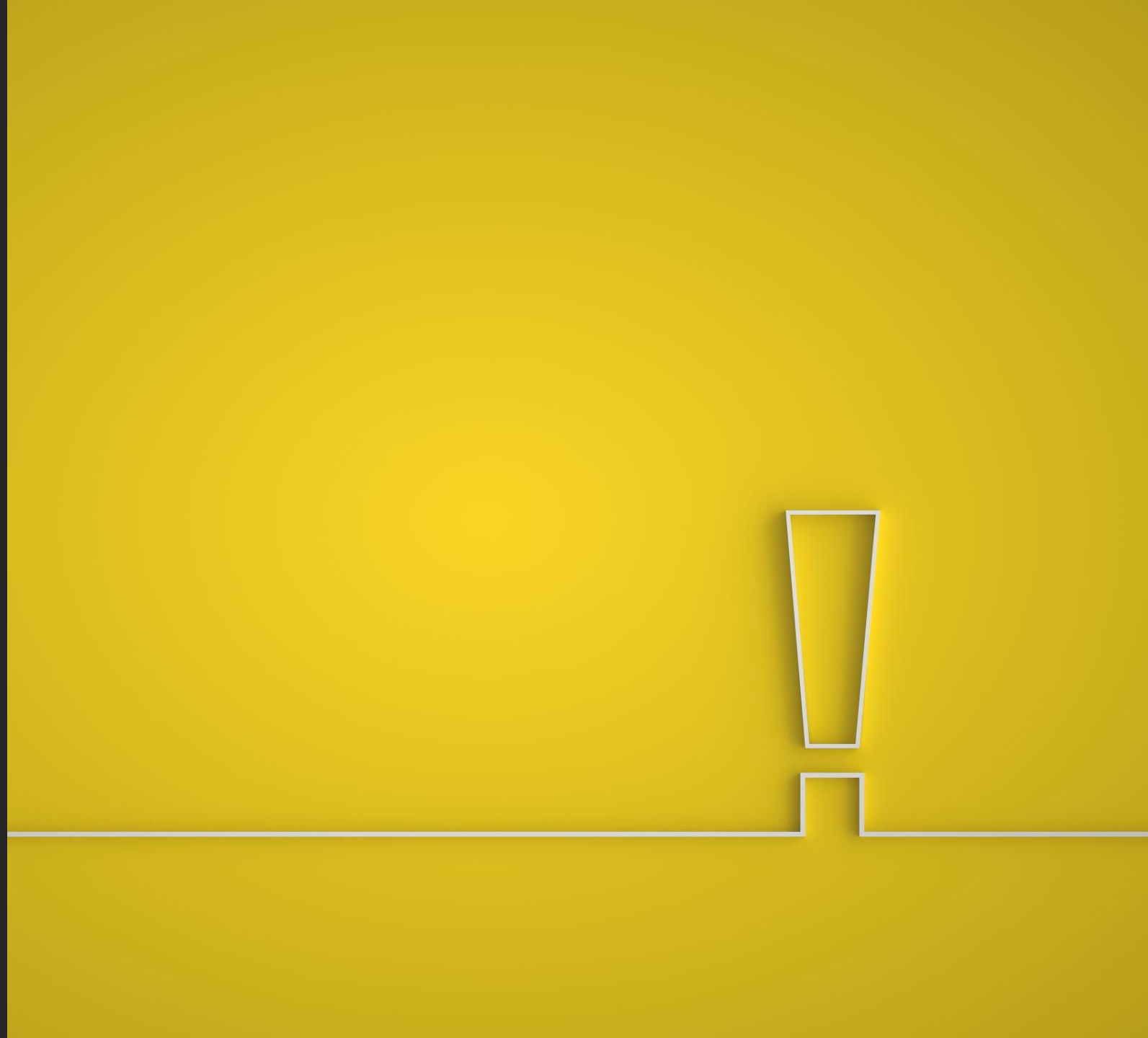
- The issue of privacy will indirectly affect the **value of disclosed information**, **whereas liability will directly affect this value.**
- While both can be interpreted as a cost and, as such, will reduce the benefit of information disclosure, privacy concerns are offset by the level of sensitivity of the information disclosed.
- Thus, while the accidental release of less-sensitive information is unproblematic, the unintended disclosure of sensitive information can result in serious liability exposure.
- These observations and relationships are represented below.

Table 2. IoT Case Studies: Privacy and Liability Considerations

	People Flow System	Eye System	Vehicle Self-Navigation System
Examples	www.xovis.com	www.google.com www.novartis.com	www.google.com www.gm.com www.mobileye.com www.tesla.com
Technology	smart sensors	smart lens	smart sensors; intelligent machine
Type of Interaction	M2M; M2H	M2H; H2M	M2M; M2H; H2M
Application	airport; train stations; entertainment venues; sport stadiums	health monitoring and health management	autonomous traffic
Value to User	medium	high	high
Value to Third Party	high	medium	high
Security Concerns	medium	high	high
Privacy Concerns	medium	high	medium
Liability	medium	high	high

Understanding this nexus between Privacy and Security and Privacy and Liability provides an added understanding of the *cost* and respective *value* of information disclosed between users (sender and direct receivers) and third parties (indirect receivers).

USE CASE...



- Categories of primary challenges and opportunities in healthcare sector versus other industries

Forces creating the biggest challenges

Healthcare sector	Global – All Industries
• Regulatory complexity	• Regulatory complexity
• Data security and privacy	• Data security and privacy
• Government policy change	• [illegible]ment policy changes
• Cost pressures	

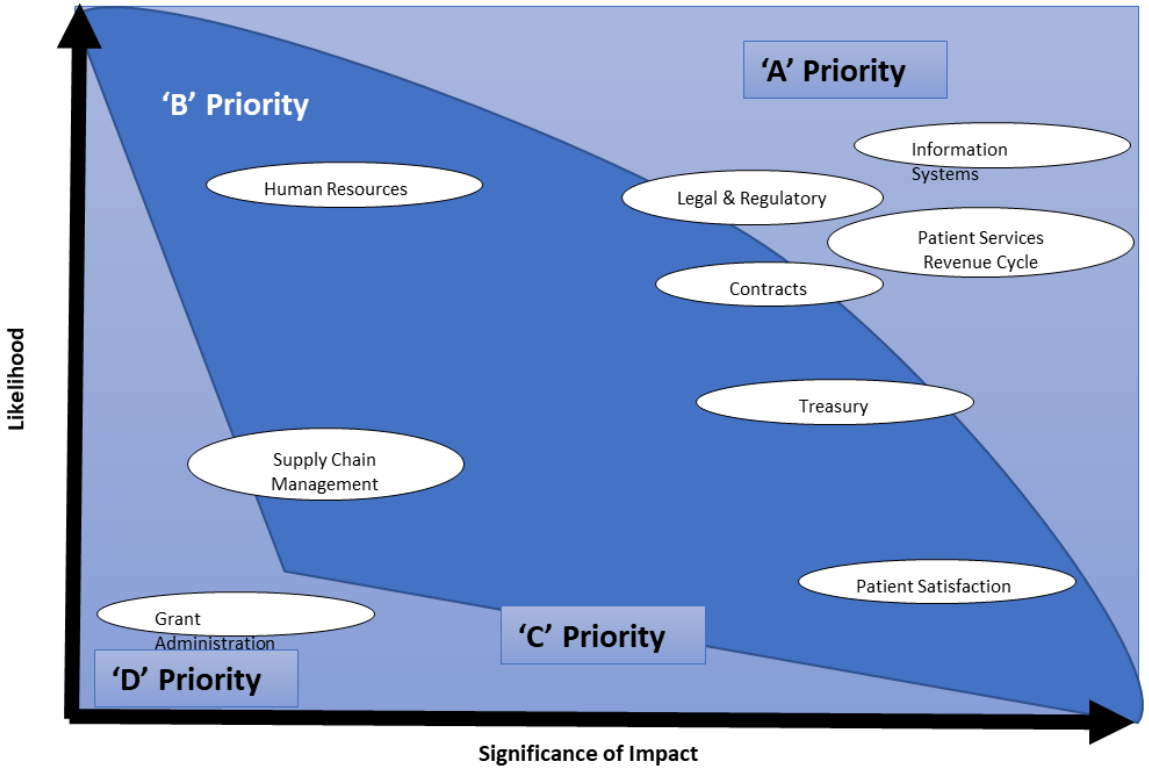
Forces [illegible]portunities

Healthcare sector	Global – All Industries
• [illegible]	• Changing consumer behavior
• [illegible] consumer / patient behavior	• Urbanization
• Shifts in competition	• Shifts in competition
• Emerging technology	• Emerging technology

This paper focusses on access to information – information asymmetry; and Identifies the need for an appropriate **approach** to solve a problem at hand concerning IoT.

INTERNAL AUDITOR FUNCTIONS WITHIN A HEALTHCARE ORGANIZATION

Function	Audit Priorities	Consequences of failing to implement
Master compliance	PPACA and ICD-10-CM 2016 compliance.	A poor ICD-10 adoption approach would result in higher denials (and, as a result, lower reimbursements), increasing accounts receivable, more intense regulatory scrutiny and diminished financial results.
Manage existing and emerging risks	Help organizations advance risk management programs, and adapt these programs to address new compliance requirements, also strengthen longstanding fraud-management capabilities.	Inability to strengthen IAs knowledge of cloud computing, data analytics and big data, resulting in stagnant control of these technologies.
Enhance Efficiency	Become more data-driven while introducing more automation to their activities in response to "do more work with less" demands.	The drive to become more effective and efficient has increased within internal audit functions.
Network and Negotiate	Learn about leading practices as they emerge, and focus on personal skills such as negotiation, and leadership.	Inability to keep up with the rapid change related to risk and compliance within healthcare.



Risk Identification within Healthcare

INFORMATION ASYMMETRY – HEALTHCARE AND THE IA

Although we have technology available….

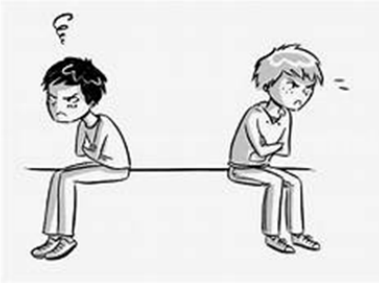
- But, it is necessary to find the specific solution that works for stakeholders so that we have the **transparency and accountability**.

What is the Approach?

- Work backwards to resolve and find an **approach**.
- It is inefficient to introduce technology for the sake of using technology.

Key questions:

- What are the **problems** (e.g. in auditing etc) that we want to solve in the first place?



- There will always be in the mix, entities with unethical behavior.
- Internal Auditors, for example, have flushed out some of such behavior.
  - E.g. Through ongoing disclosure requirements.

There is a need for accounting professionals to better understand the role of **information asymmetry** and granularity in organizations and therein the intercept of the IoT and stakeholder value in the new MIS.

FAIRNESS AND INFORMATION ASYMMETRY

- In implementing IoT into organizations, it is necessary to take into account perceived fairness and equality.

We have information asymmetry between stakeholders, and there are both benefits and drawbacks of this collaboration.

ITEMS REQUIRED TO BE REPORTED ON AN 8-K REPORT

Section	Item	Problematic identification of trigg event
ction 1 egistrant's Business d Operations	**Item 1.01:** Entry into a Material Definitive Agreement **Item 1.02:** Termination of a Material Definitive Agreement **Item 1.03:** Bankruptcy or Receivership **Item 1.04:** Mine Safety - Reporting of Shutdowns and Patterns of Violations	
ction 2 nancial formation	**Item 2.01**: Completion of Acquisition or Disposition of Assets **Item 2.02:** Results of Operations and Financial Condition **Item 2.03:** Creation of a Direct Financial Obligation or an Obligation under an Off-Balance Sheet Arrangement of a Registrant **Item 2.04**: Triggering Events That Accelerate or Increase a Direct Financial Obligation or an Obligation under an Off-Balance Sheet Arrangement **Item 2.05:** Costs Associated with Exit or Disposal Activities **Item 2.06**: Material Impairments.	**Item 2.06**: Material Impairments.
ction 3 curities and ading Markets	**Item 3.01:** Notice of Delisting or Failure to Satisfy a Continued Listing Rule or Standard; Transfer of Listing **Item 3.02:** Unregistered Sales of Equity Securities **Item 3.03:** Material Modification to Rights of Security Holders	
ction 4 atters Related to countants and nancial Statements	**Item 4.01:** Changes in Registrant's Certifying Accountant **Item 4.02:** Non-Reliance on Previously Issued Financial Statements or a Related Audit Report or Completed Interim Review	
ction 5 rporate overnance and anagement	**Item 5.01:** Changes in Control of Registrant **Item 5.02**: Departure of Directors or Certain Officers; Election of Directors; Appointment of Certain Officers; Compensatory Arrangements of Certain Officers **Item 5.03:** Amendments to Articles of Incorporation or Bylaws; Change in Fiscal Year **Item 5.04:** Temporary Suspension of Trading Under Registrant's Employee Benefit Plans **Item 5.05:** Amendment to Registrant's Code of Ethics, or Waiver of a Provision of the Code of Ethics **Item 5.06:** Change in Shell Company Status **Item 5.07:** Submission of Matters to a Vote of Security Holders **Item 5.08:** Shareholder Director Nominations	
ction 6 set-Backed curities	**Item 6.01:** ABS Informational and Computational Material **Item 6.02:** Change of Servicer or Trustee **Item 6.03:** Change in Credit Enhancement or Other External Support **Item 6.04:** Failure to Make a Required Distribution **Item 6.05:** Securities Act Updating Disclosure	
ction 7 egulation FD	**Item 7.01:** Regulation FD Disclosure	
ction 8 ther Events	**Item 8.01:** Other Events (The registrant can use this Item to report events that are not specifically called for by Form 8-K, that the registrant considers to be of importance to security holders.)	**Item 8.01:** Other Events (registrant can use this Iten report events that are not specifically called for by Form 8-K, that the registra considers to be of importa to security holders.)
ction 9 nancial Statements d Exhibits	**Item 9.01:** Financial Statements and Exhibits	

CONCLUDING COMMENTS

- This study explored whether and the extent to which the IoT has changed and continues to change the design of MIS in organizations, including but not limited to the accounting profession in the COVID-19 environment, that are using the IoT.
  - First, this study contribute to the IS theory-building literature by developing a theoretical framework in the context of the IoT.
    - The model showed that **when privacy and liability concerns are classified as costs**, the **value of information disclosure** can be reduced.
  - Second, decision making by managers and its impact on the strategic advisory role (accounting profession) and healthcare.
  - Third, this paper contributes to the MIS design literature by moving the "new" MIS to the periphery.
    - In particular, the author shows how the placement at the AI machine-level can mitigate privacy and potential liability concerns of organizations operating within the domain of the IoT and how such MIS can serve both humans and AI machines.

THANK YOU!

Dr. Sarah Hinchliffe

LLB(Hons)(Monash), LLM(Tax)(UNE), MSA (Akron), PhD(VU), AIIFL Honorary Fellow (HKU)
Barrister & Solicitor (High Court of Australia, Victorian Supreme Court), Registered Migration Agent
Chartered Tax Advisor, Tax Agent (Australia), Chartered Accountant

Email: sarah.Hinchliffe@hotmail.com

QUESTIONS