A FRAMEWORK FOR UNIFIED PRIVACY MANAGEMENT

BEYOND CONSENT

KEVIN L. MILLER

LABYRINTH RESEARCH

Robotics Privacy Research

Software Engineer / Architect

Registered Patent Attorney

Cybersecurity & Privacy Attorney

Juris Doctor from the University of Florida

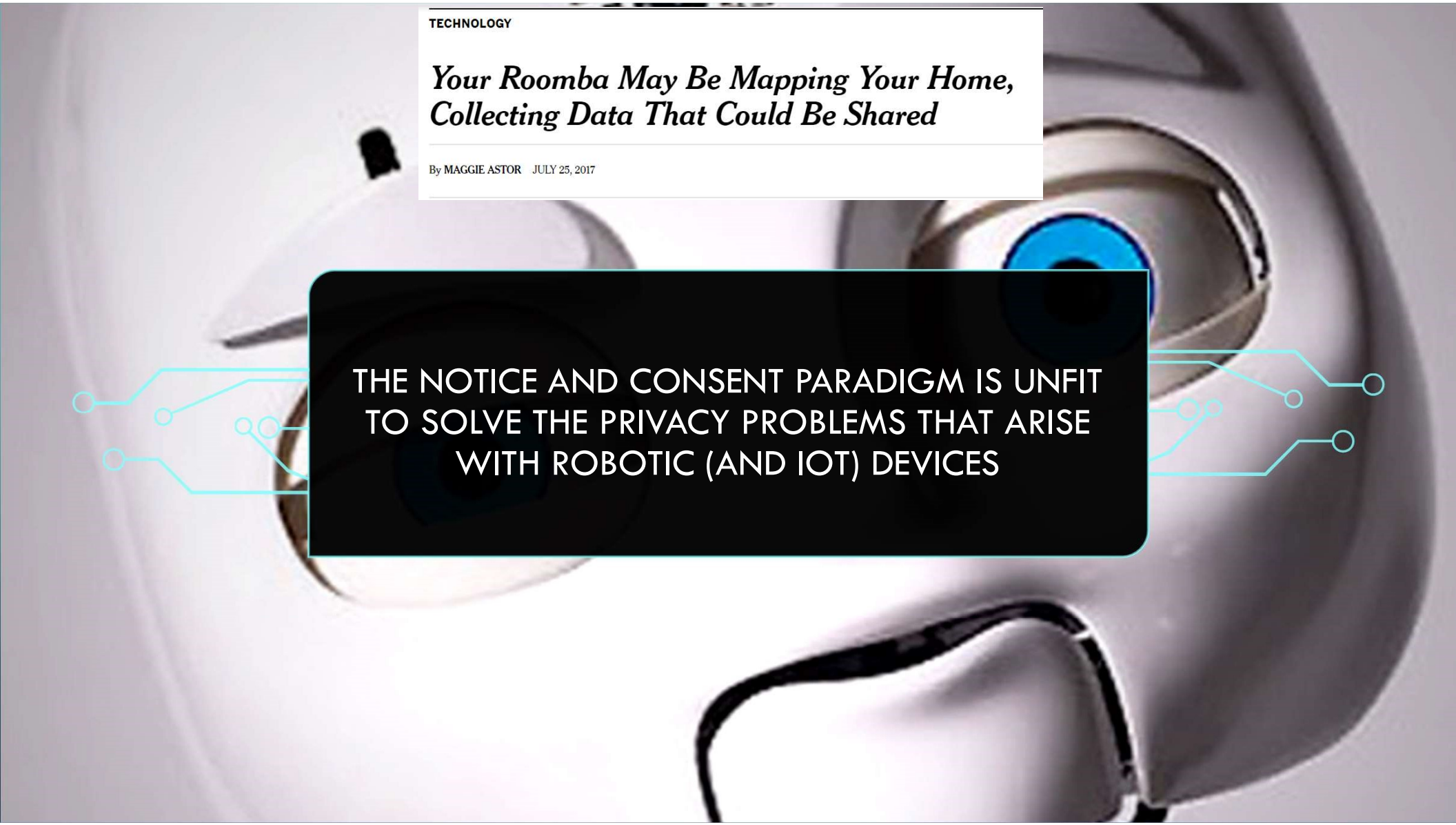
M.B.A. in Technology Management

Microsoft Certified Solutions Developer (MCSD)

THE CURRENT PARADIGM OF PRIVACY IS DEFINED BY "NOTICE AND CONSENT"

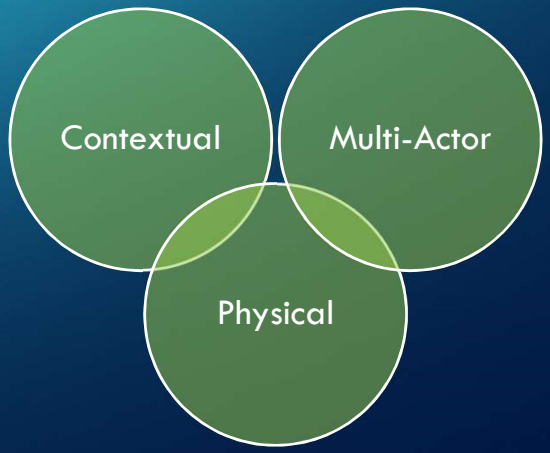
Business presents user a broad "privacy" notice and asks for their consent to collect personal information and behavioral data in return for "free" use of app/service.

Privacy protection in all spheres gradually erodes because users now "expect" their data to be sold


TECHNOLOGY
Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared
By MAGGIE ASTOR JULY 25, 2017
THE NOTICE AND CONSENT PARADIGM IS UNFIT TO SOLVE THE PRIVACY PROBLEMS THAT ARISE WITH ROBOTIC (AND IOT) DEVICES

ROBOTICS PRIVACY IS QUALITATIVELY DIFFERENT FROM APP/SERVICE PRIVACY

- Robots have *many* sensors for recording activities of people around them
- Robots are mobile (they can autonomously move into different spaces inhabited by different people at any time)
- Robots make physical contact with us (sometimes in ways that might be disturbing)
- Privacy expectations are based on cultural norms, shared group values, and even on current location
  - Situational contexts such as an emergency may override all other concerns



RE-ENVISIONING PRIVACY FROM A CYBERNETIC VIEWPOINT

OBJECTIVE	Ensure that robot control functions—namely, sensor activation and recording, as well as movement and action—meet the contextually sensitive privacy expectations of individuals coinhabiting the robot's zone of influence
CONTEXTUAL PRIVACY	Use legal and sociological understandings to design a model that exposes systematic assumptions and neutrally adopts norms to account for cultural and contextual subtleties
FRAMEWORK	Develop a technical architecture to align command and control of robots with human expectations in an environmental context

1

PRIVACY IDENTITY DETECTION AND PREFERENCE EXCHANGE

Robots need to know the "privacy identity" of individuals in their zone of influence

Robots need data about the privacy expectations of these individuals

PERSONAL PRIVACY DEVICE (PPD) ACTS AS A "BEACON"

OUTSIDE SENSOR RANGE

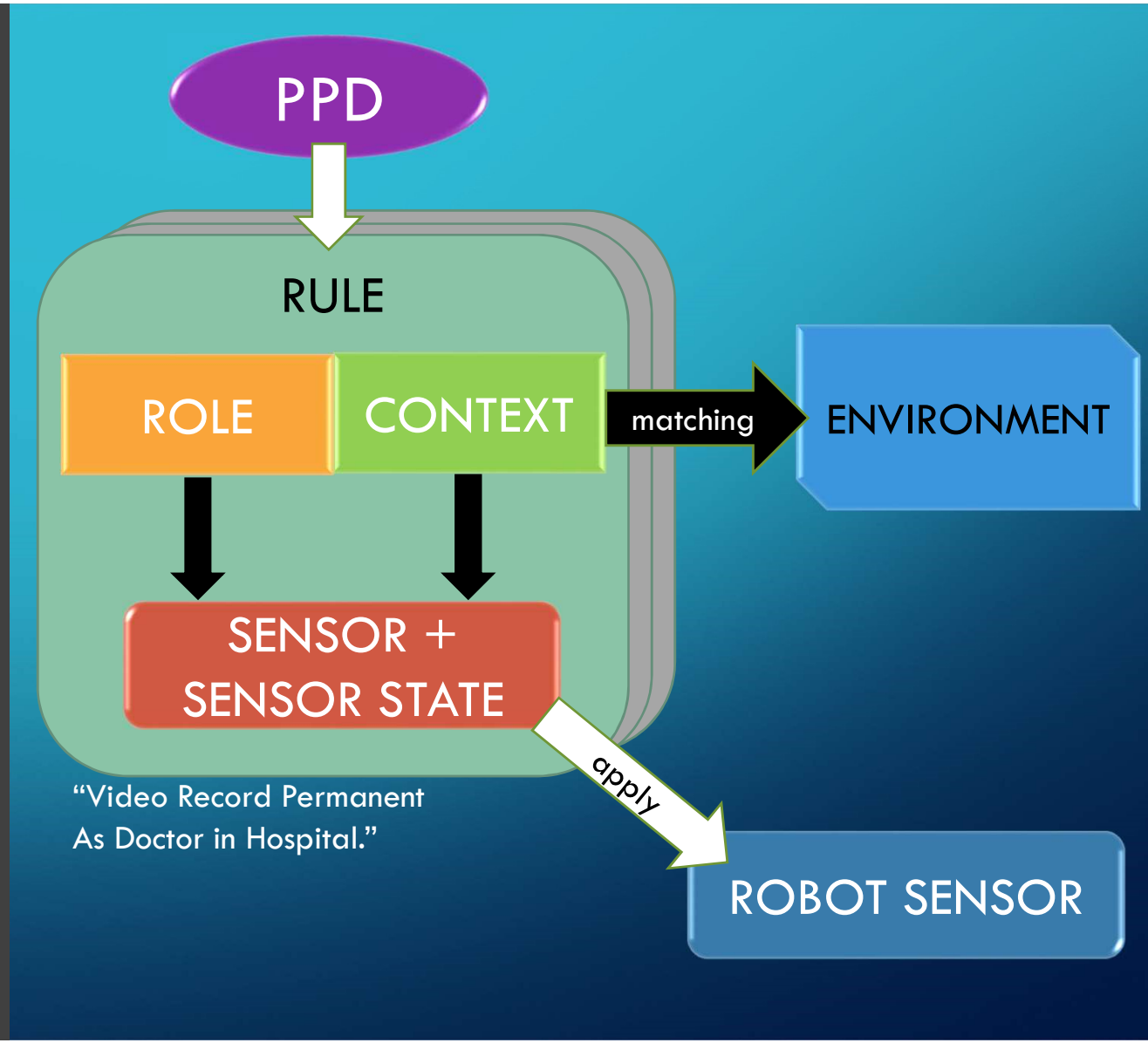
ROBIOTA ZONE
INSIDE SENSOR RANGE
(E.G. 100 METERS)

OUTSIDE SENSOR RANGE

2

PRIVACY RULES/ TAXONOMY

What is
"privacy preference data"?



TAXONOMY CONTINUED…

Role examples (Kathy as doctor and patient)

- "Video Record Permanent As Doctor in Hospital."
- "Video Orient-Only As Patient in Hospital."

Person	Sensor	Sensor State	Role	Context
P1	Video	Orient Only	Friend	Other's House
P2	Video	Record Persist	Me	My House
P1	Video	Orient Only	Patient	Hospital
P2	Video	Record Persist	All	Public Place

Context Layer	Notes and Example Taxa
Cultural	Cultural background of a region, religious affiliation, ethnic group
Societal	Economic system, political structure
Group	Voluntary or involuntary affiliation with a societal segment or group, such as charity, church, advocacy group, support group, political affiliation, formerly incarcerated
Locational	Home, place of employment, private meeting, friend's house, medical facility, region, country, state, city, country
Individual	Pertains to the individual or collective owner of a privacy identity
Situational	Ad hoc situations, emergencies or times when security or safety of self/others is impacted
Legal	Constitutional, statutory, or regulatory constraint, e.g., compliance with a privacy law or judicial/law enforcement rule of conduct
Trust Relationship	Explicit or implicit interaction relationship with the robot entity, such as a robot one personally owns or that inhabits a place of employment; functional relationship, such as a personal care robot

PROCESSING PROTOCOL FOR ROBOT CONTROL FUNCTIONS

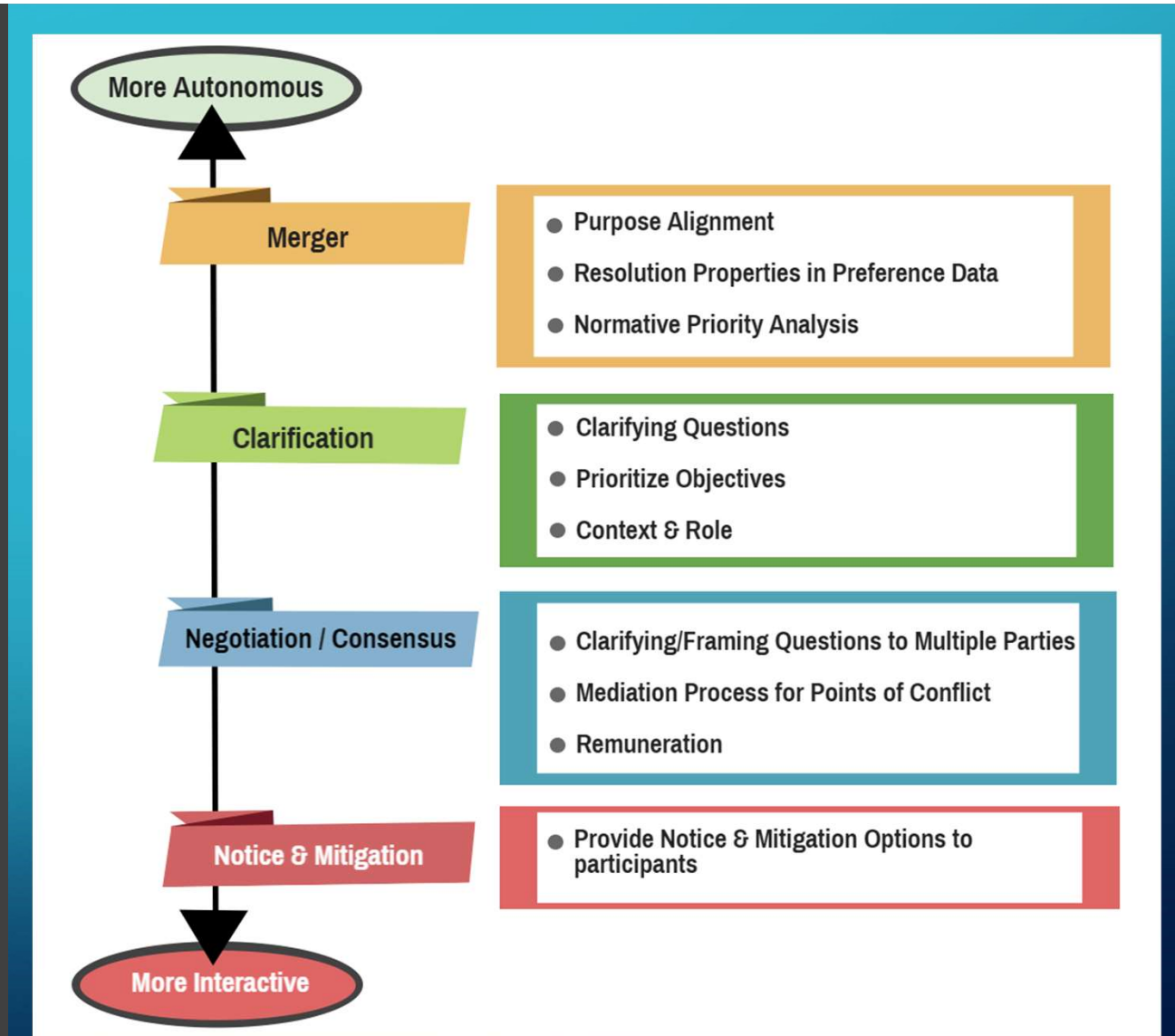
Protocol 1: Basic processing protocol for privacy preference framework interactions.

Require: R, a robot; S_R, the robot sensor array

1: ENUNCIATORS $E \leftarrow get\_enuciators\_within\_detection\_range\,(R)$
2: PRIVACY-IDENTITIES $P \leftarrow get\_privacy\_identities\_from\_enunciators\,(E)$
3: OPERATING-CONTEXT $c_{op} \leftarrow get\_current\_operating\_context\,(R)$
4: **for each** PRIVACY-IDENTITY $p \in P$ **do**
5: VECTOR $d_p \leftarrow determine\_vector\,(E_p)$
6: ROLE $r_p \leftarrow query\_privacy\_identity\_role\,(p, c_{op})$
7: **for each** SENSOR-CONTROL $s \in S_R$ **do**
8: CONTROL-RANGE $sr_s \leftarrow query\_control\_range\,(s)$
9: **if** $within\_control\_range\,(sr_s, d_p) =$ true **then**
10: RULE $y_{p,s} \leftarrow retrieve\_rule\_from\_hierarchy\,(p, s, c_{op}, r_p)$
11: RULE-SET $Y \leftarrow add\_composite\_rule\_set\,(y_{p,s})$
12: **end if**
13: **end for**
14: **end for**
15: RULE-CONFLICTS $Y_c \leftarrow validity\_check\,(Y,$ "conflict")
16: **for each** RULE-CONFLICT $y_c \in Y_c$ **do**
17: CONTROL-STATE $t_y \leftarrow resolve\_conflict\,(y_c)$ //see Merger Protocol
18: $apply\_control\_state\,(t_y)$
19: **end for**
20: RULE-SET $Y_{ok} \leftarrow validity\_check\,(Y,$ "no-conflict")
21: **for each** RULE $y_{ok} \in Y_{ok}$ **do**
22: CONTROL-STATE $t_y \leftarrow get\_control\_state\_from\_rule\,(y_{ok})$
23: $apply\_control\_state\,(t_y)$
24: **end for**
25: $Log\_outcomes\,(Y_c, Y_{ok}, P, c_{op}, time)$

3

MERGER AND RESOLUTION OF PREFERENCE CONFLICTS



Purpose Alignment

Examines the robot's purpose in the environment

Will the conflict block a specific robot activity that relates to the robot's reason to be there? How necessary is that specific activity to the robot's overall purpose?

Normative Priority Analysis

Expressed hierarchy of priority ingrained in cultural context

Hierarchy allows conflict resolution by giving priority to certain rules over others

- Examples: majority wins, prefer family over friends, do the least harm to most people, a parent's rules supersede her minor child, law enforcement drone looking for fugitive outranks conflicting privacy expectations

Side effect: a way of expressing and dealing with society's implicit biases

Clarifying Questions

Robot interacts with at least one actor in the detection zone for more information:

- An actor's goals or priority of objectives
- An unclear context
- An unclear role

Multiple Parties	Multi-actor clarifying and "framing" questions ("frame" the conflict so that underlying presuppositions about the context or other matters are made apparent to the human actors)
Mediation	Robot engages in mediation process with the conflicting actors to in which one person voluntarily yields priority to another
Remuneration 	Attempt to reward consensus when unable to mediate a conflict ▪ Robot can impart a tangible benefit on actors who cannot agree ➢ Micropayments ➢ Privacy credits given to actor who yielded and taken from the actor who received priority ➢ Blockchain architecture could facilitate

Notice & Mitigation

- All other attempts have failed
- Robot determines “best” final control state (in light of normative rules above)
- Provide notice to person whose privacy expectations were unavoidably subjugated
- Suggest mitigating actions (“leave the room”)

4

ACCOUNTABILITY: LOGGING AND AUDIT

- Facilitates transparency in autonomous systems
- Logging of
  - context and role inputs
  - actors and their preferences
  - the answers to clarifying questions
  - negotiation outcomes
  - final control state selections
- Documents when consent was given during consensus negotiation if needed for legal purposes
- Random audit of inputs ⟹ control state helps ensure that robots process privacy preferences in accordance with framework

BLOCKCHAIN + SMART CONTRACTS

- Platform backbone for privacy settings exchange and negotiation/consensus protocols (including remuneration models).
  - Mitigates weaknesses of centralized model with single privacy settings provider
  - Distributed storage and processing architecture for privacy preference data
  - Transparency/Accountability
    - Complete formal system for rule processing reduces ambiguity in outcomes
    - Outcomes can be audited without exposing individual privacy identities when built on variable permission structures of smart contracts

SOCIETY AND POLICY STAND TO GAIN FROM AN APPROACH ENABLING A RENEWED CONCEPTION OF PRIVACY

- Re-centers privacy on the individual by enabling fine-grained choices about privacy expectations reflecting personal and cultural values
- Re-energizes the legal conversation about the "reasonable expectation" of privacy and moves the reasonableness threshold in a positive direction
- Turns consent on its head
- Remuneration model for resolution of conflicts: the rewards for subverting our privacy goals accumulate to individuals, rather than to ad networks and big data brokers.

- The contextually-neutral normative analysis, value judgments, and rule hierarchies encodes evaluative and processing constructs in a way that exposes hidden assumptions and biases

CONTACT INFO

Kevin L. Miller

Labyrinth Research

klmiller@labyrinth-research.com