Internet Policy Research Initiative

NAS Workshop: Opportunities for Accelerating Scientific Discovery: Realizing the Potential of Advanced and Automated Workflows

Challenges of Policy-Aware Data Processing

March 17, 2020 - via Zoom

Daniel J. Weitzner weitzner@mit.edu, MIT IPRI Founding Director

Challenges of Policy-Aware Data Processing

- Legibility of Rules
- Scalability, Federation and Modularity
- Accountability Behavior

Policy Soundness and Technical Completeness

- Policy Soundness: How do we develop systems that can be shown to be logically sound with respect to a set of policy goals?
  - Computer Science question
  - Guidance from law and policy experts required
  - Easier with deterministic systems
- Technical Completeness: How can we tell when a policy ruleset or governance mechanism is complete with respect to the capabilities of a technical system?
  - Legal/policy question
  - Requires insight from Computer Science

Incommensurability of Computer Science and Law

What does it mean for a system to ‘work’?

- *Computer science*: tech system works when...
  - provide a fully specified, correct solution to a well defined and well understood problem
  - implemented and maintained according to sound engineering practice.
- *Law:* legal system works when constituent rules are...
  - proper expressions of the society’s values
  - have the necessary indicia of legitimacy

Feigenbaum, Joan, and Daniel J. Weitzner. "On the incommensurability of laws and technical mechanisms: Or, what cryptography can’t do." In Cambridge International Workshop on Security Protocols, pp. 266-279. Springer, Cham, 2018.

Rule of Law = rules + principles

Rules: logical propositions that are expected to yield answers about what is and is not permitted using formal reasoning capabilities

Principles: articulate values and policies that must be reflected in a legal system but do not necessarily dictate an unambiguous outcome in any given case

R. Dworkin, Taking Rights Seriously, Harvard University Press, Cambridge MA, 1978.

Example: How rules and principles work together (1)

Rule: If a person dies intestate, then her estate is passed down to her spouse and any surviving children.

Principle: No one shall be permitted to profit from his own fraud.

Example: How rules and principles work together (2)

Rule: Caveat emptor protects car manufacturer from paying damages for unwarranted uses.

Principle: In a society with such significant reliance on automobiles, the car manufacturer is under a “special obligation with respect to the construction, promotion and sale of his cars.”

Rules and Principles in Digital Rights Management Systems

DRM systems designed to provide ease of access but no unlicensed copies

Rule: Exclusive rights to make copies of works of authorship

Principle: Fair use as free-expression-grounded exception, sometimes justifying intrusion on exclusive rights.

Implementing Privacy: policy and tech challenges - unsolved problems

GDPR	Consumer Privacy Bill of Rights	Cal. Consumer Privacy Act	Apple proposal
Lawful basis - Consent, etc.	Right individual control		
legitimate interest,etc	Right to respect for context	Rig	
Right to be informed	Right to transparency	Right to kno	Right to know
Right of access	Right to acc		Right to access
Right to rectification	Right to accu		
Right to erasure		Ri d deleted	
Right to restrict processing		[illegible] discrimination for exercise	Right to minimization
Right to portability	Machine		
Right to object	Right to c		
Right to avoid automated decisionmaking & explanation			
Data Breach Notification	Security & Breach Notification		rity
Accountability	Accountability		
Fines < 4% annual revenue	Fines	$7500/incident, 30 day cure	

Art. 5 GDPR

rsonal data

Processing shall be lawful only if and to the exter he following applies:

1. t has given consent to the processing of his or her personal data for one or **urposes**;
2. ecessar nce of a contract to which the data subject is party ke step f the data subject prior to entering into a contract;
3. with a legal obligation to which the controller is subject;
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person;

is necessary for the performance of a task carried out in the public interest or in e of official au e controller;

is necessary f the **legitimate interests pursued** by the such interests are overridden by the interests or fundamental rights and fr a subjec tion of personal data, in particular where the data subject is a child.

Purpose limitation enforcement

Effective Notice - HCI/UX

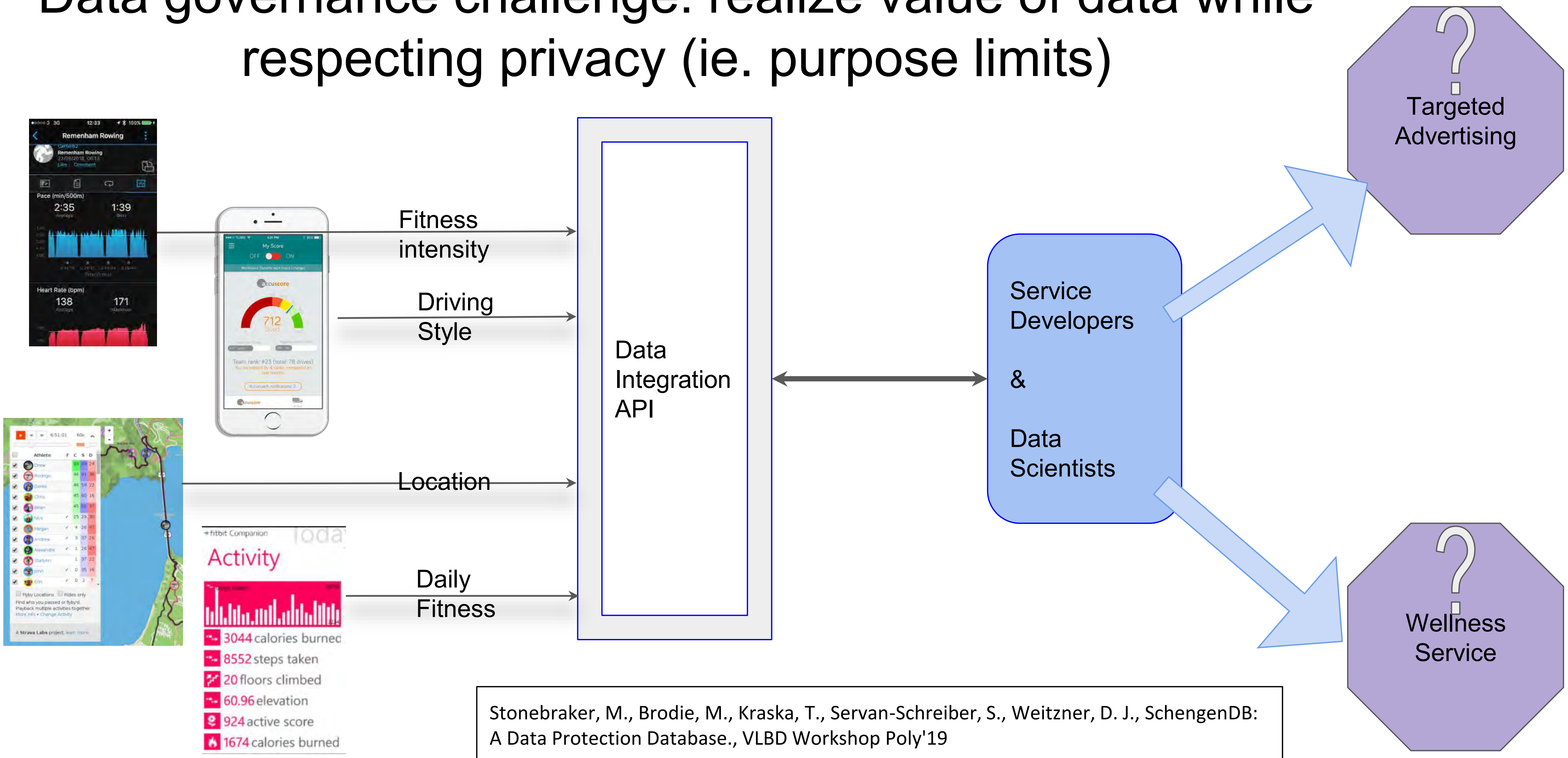
Hard Delete

Graph privacy

ML explanation

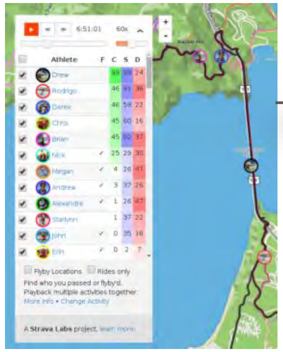
Policy-Aware Event Logging

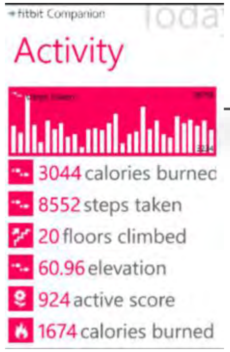
Data governance challenge: realize value of data while respecting privacy (ie. purpose limits)



Stonebraker, M., Brodie, M., Kraska, T., Servan-Schreiber, S., Weitzner, D. J., SchengenDB: A Data Protection Database., VLBD Workshop Poly'19

Traditional approach: access control




fitbit Companion

Today

Activity

3044 calories burned

8552 steps taken

20 floors climbed

60.96 elevation

924 active score

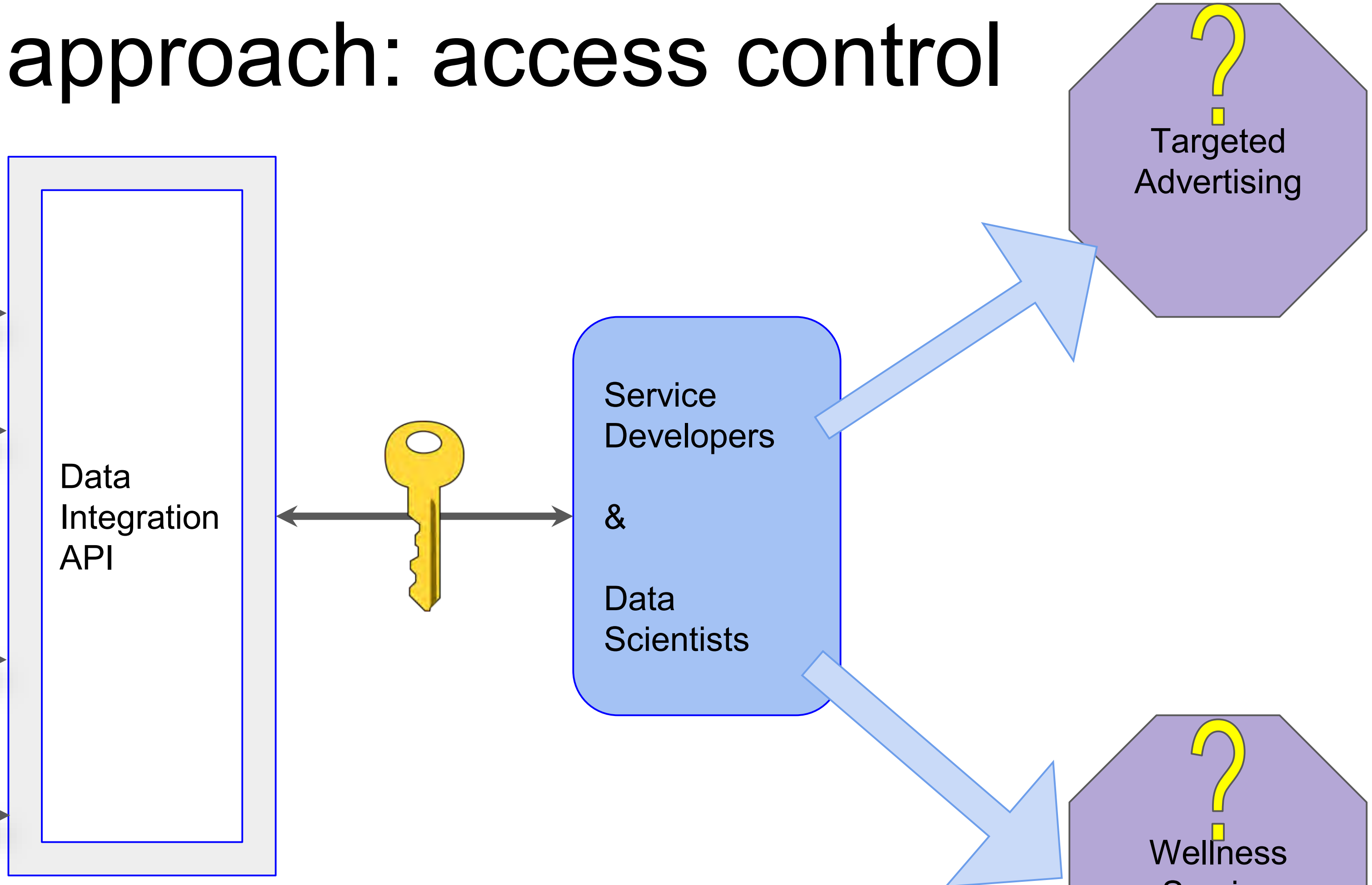
1674 calories burned

Fitness intensity

Driving Style

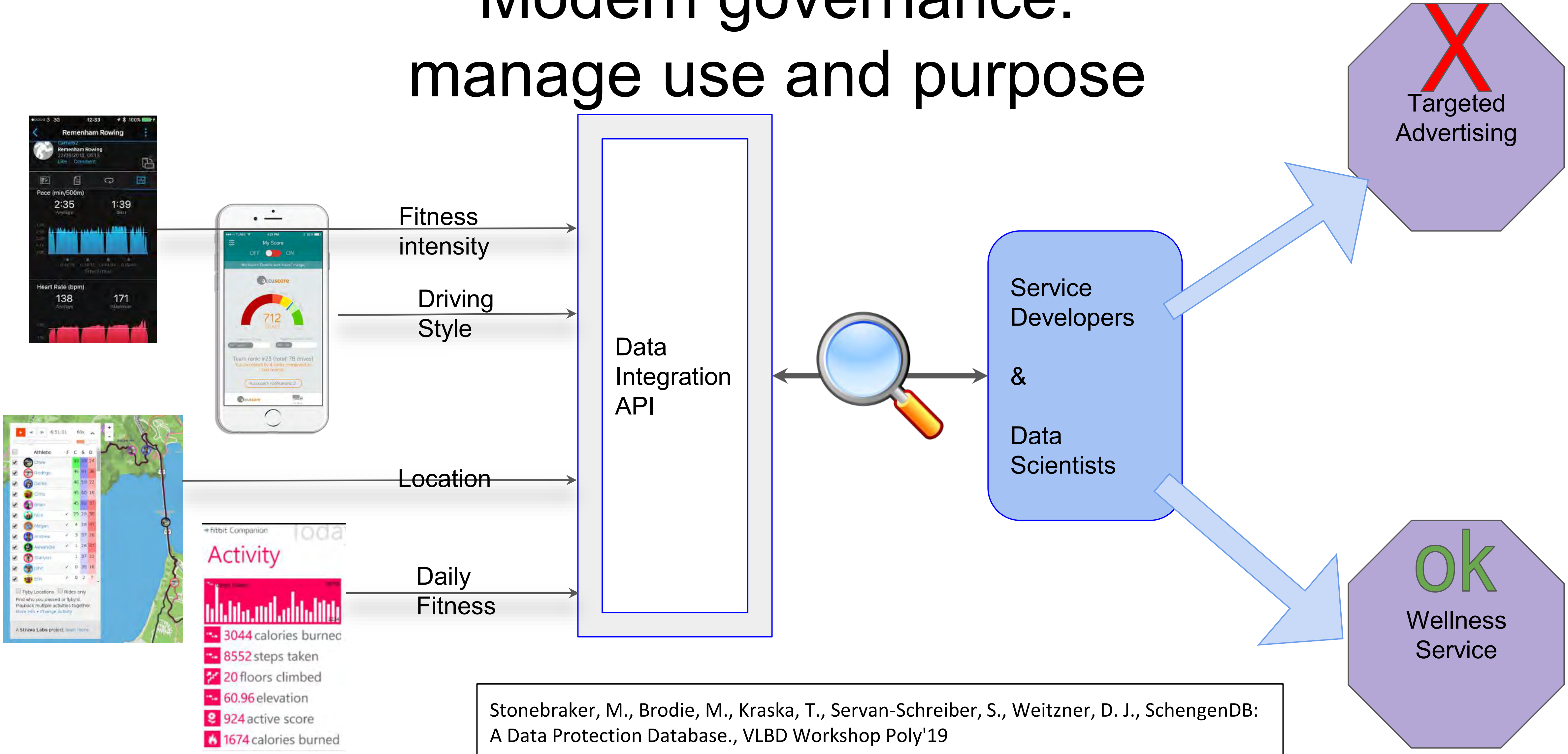
Location

Daily Fitness



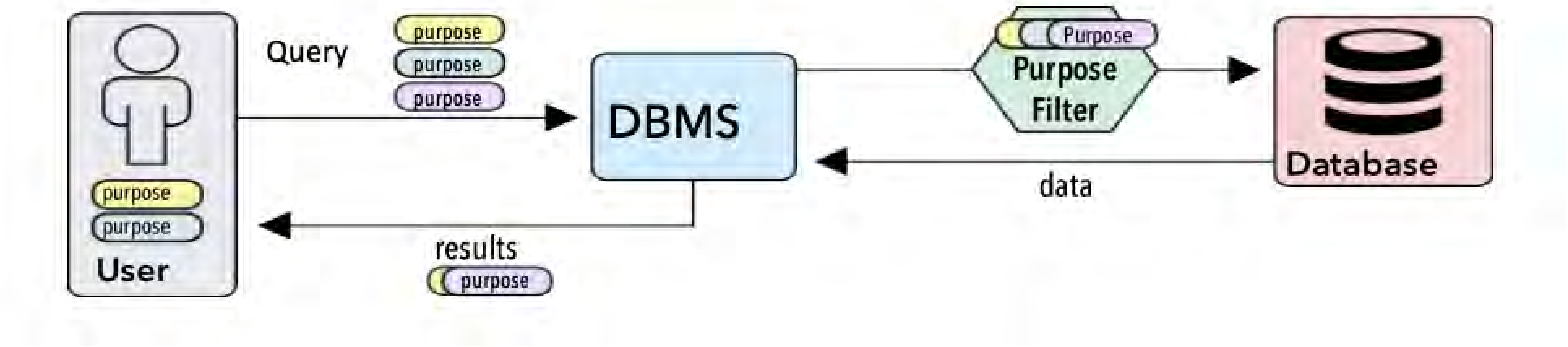
Stonebraker, M., Brodie, M., Kraska, T., Servan-Schreiber, S., Weitzner, D. J., SchengenDB: A Data Protection Database., VLBD Workshop Poly'19

Modern governance: manage use and purpose



Stonebraker, M., Brodie, M., Kraska, T., Servan-Schreiber, S., Weitzner, D. J., SchengenDB: A Data Protection Database., VLBD Workshop Poly'19

Purpose-Aware Database Architecture



Stonebraker, M., Brodie, M., Kraska, T., Servan-Schreiber, S., Weitzner, D. J., SchengenDB: A Data Protection Database., VLBD Workshop Poly'19

Design Patterns to Bridge the Incommensurability Gap

#1 - Law: Reduce Gray Area between rules and principles

- Enables assessment of policy soundness and technical completeness

#2 - Tech: Avoid designs that makes automated and non-transparent decisions when principles are at stake.