Haojian Jin

What we have covered.

- Location privacy
- Permissions for Privacy
- Policies for Privacy

Privacy Conceptual Framework

- What is Privacy?
- How to justify privacy?

Privacy Conceptual Framework

- Contextual Integrity (Appropriate information flow)
- Approximate Information Flow
- Traditional (private v.s. public places)
- Fair information principles
- Alan Westin, Privacy and Freedom, 1967.

3,652,539 views | Feb 16, 2012, 11:02am

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Former Staff
Tech
Welcome to The Not-So Private Parts where technology & privacy collide

This article is more than 2 years old.

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT +0%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

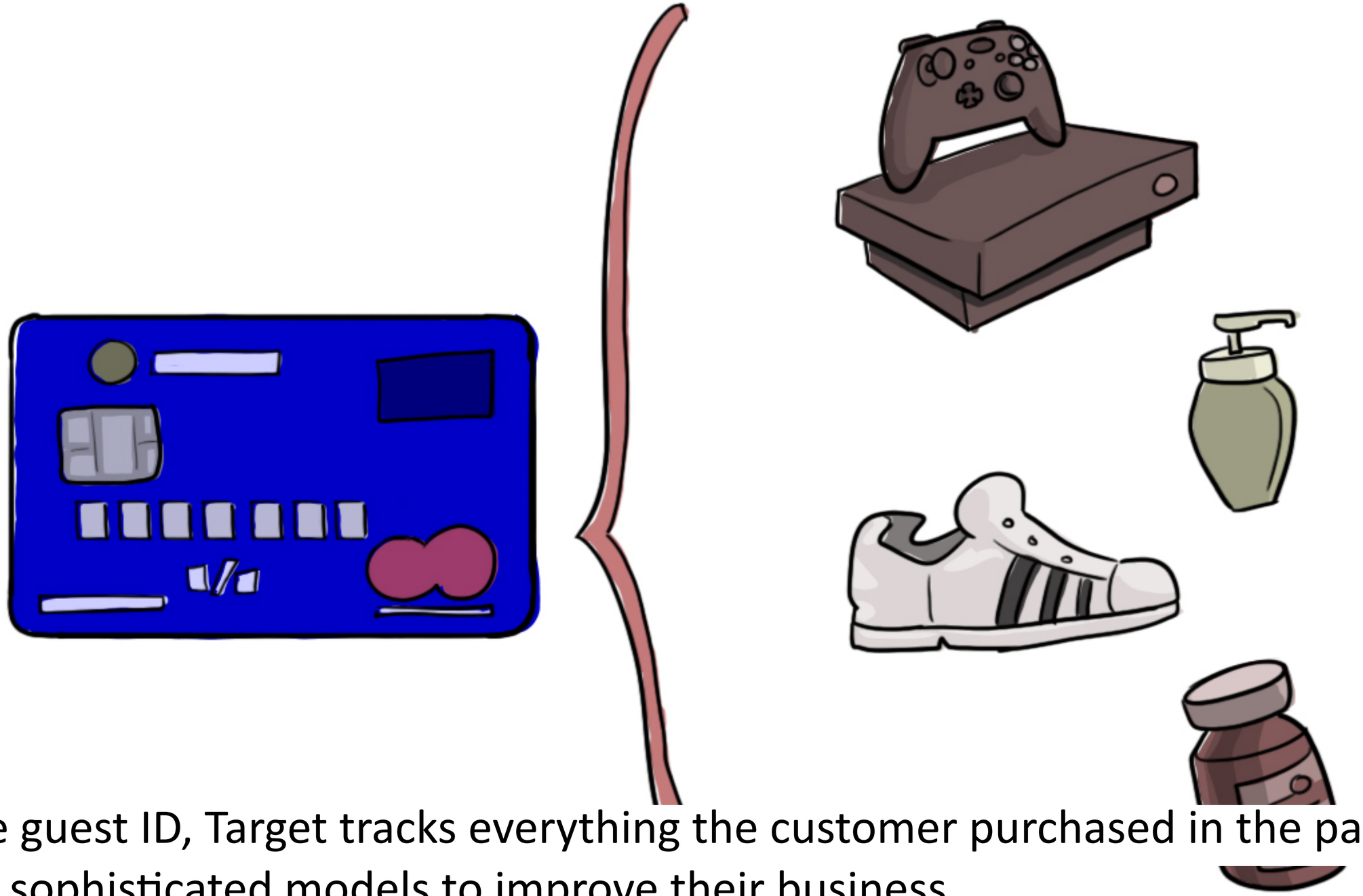
TARGET

Target has got you in its aim

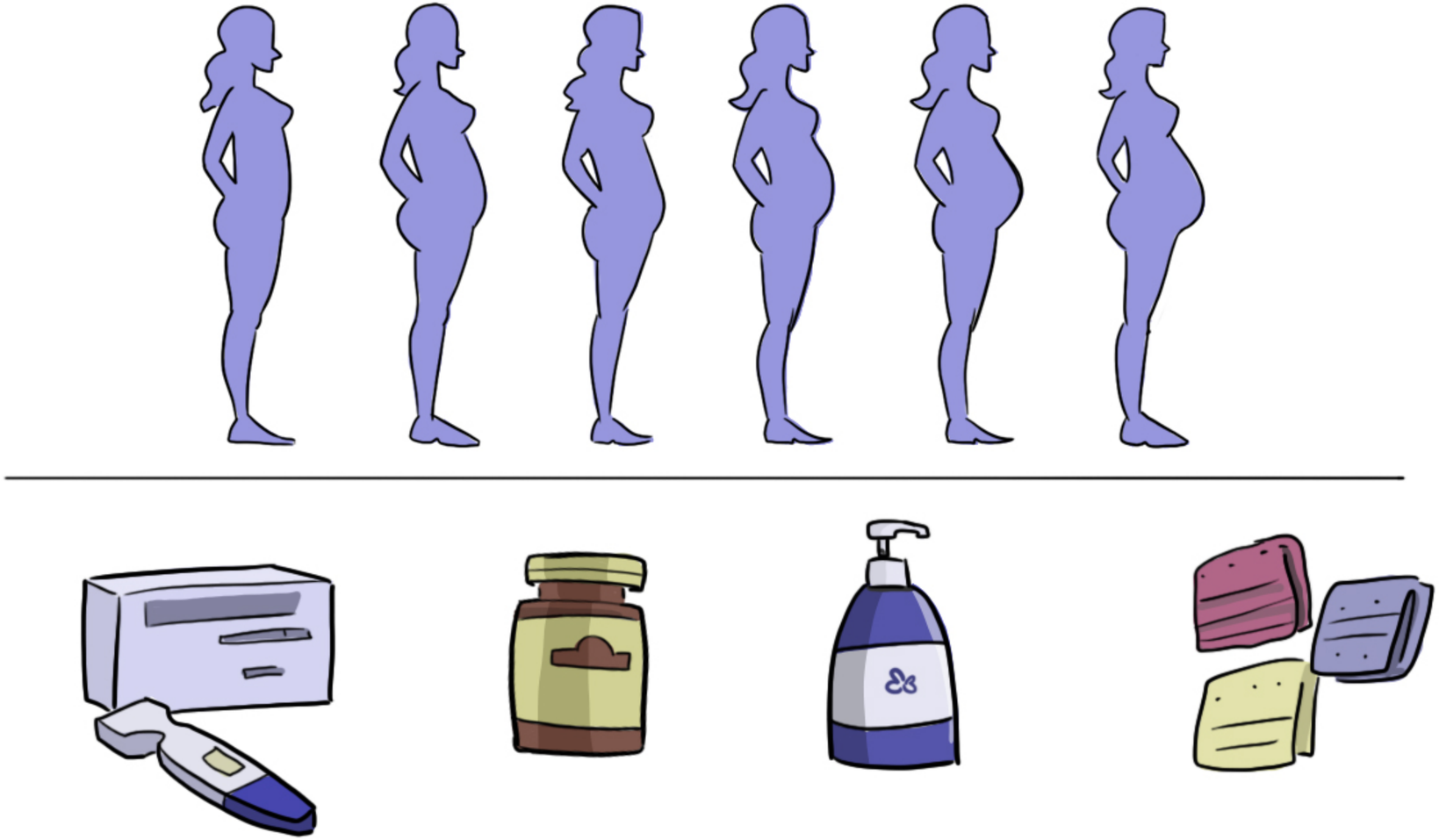
Target predicted that a teenage girl might be pregnant and sent a diaper coupon to the girl.

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.
Kashmir Hill, Forbes, 2012

Target assigns every customer a guest ID number, tied to their credit card, name, or email address and collects their demographic information through various channels.



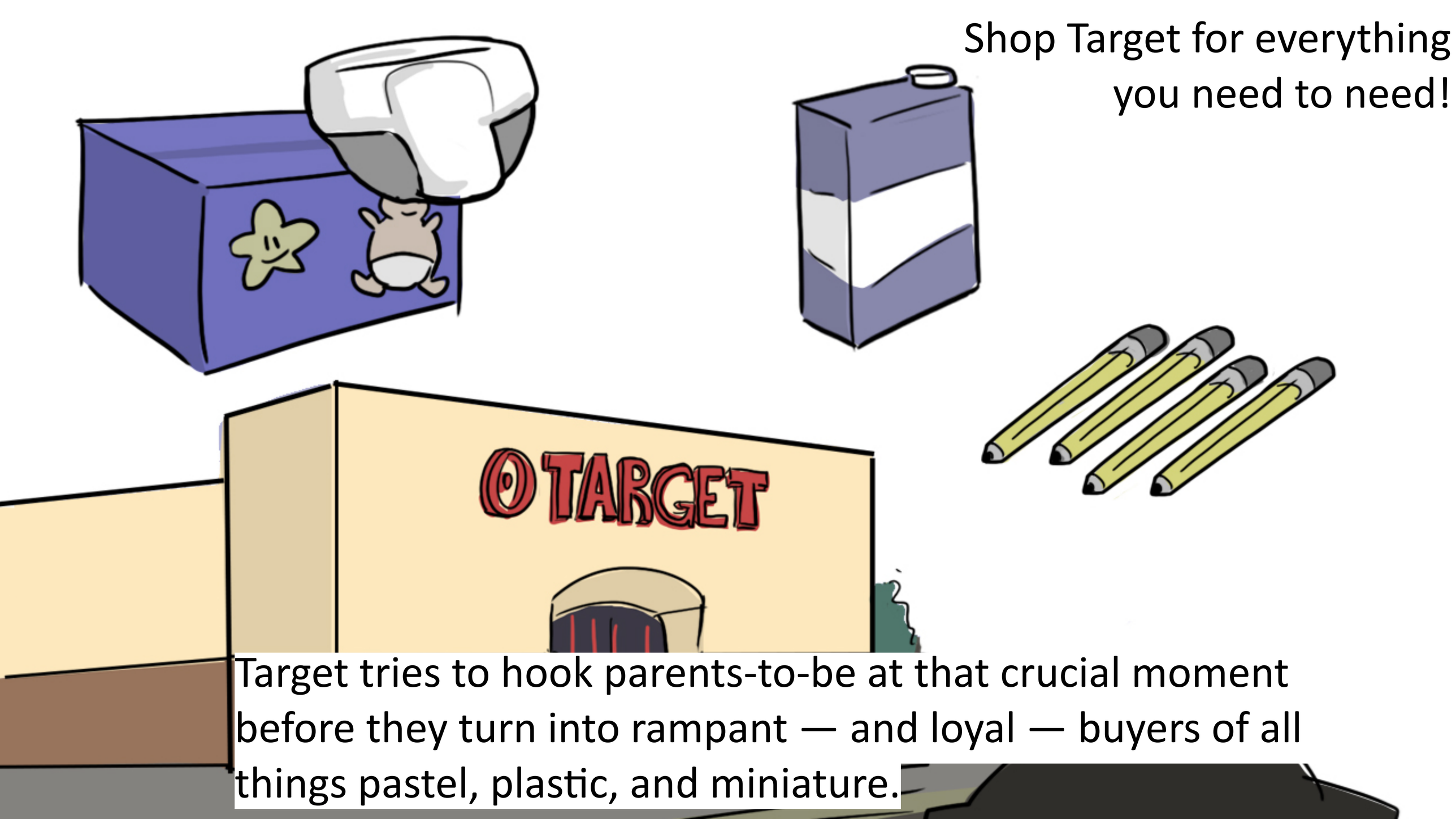
Using the guest ID, Target tracks everything the customer purchased in the past and develops sophisticated models to improve their business.



Pregnant women purchase different items during the gestation period. For example, sometime in the first 20 weeks, pregnant women loaded up on supplements like calcium, magnesium and zinc.

Target will send coupons for baby items to customers according to their pregnancy predictions.


The reason behind it is that research shows that frustrated first time parents are more likely to change their lifelong shopping behavior during the overwhelming period.


Shop Target for everything you need to need!
TARGET
Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and loyal — buyers of all things pastel, plastic, and miniature.

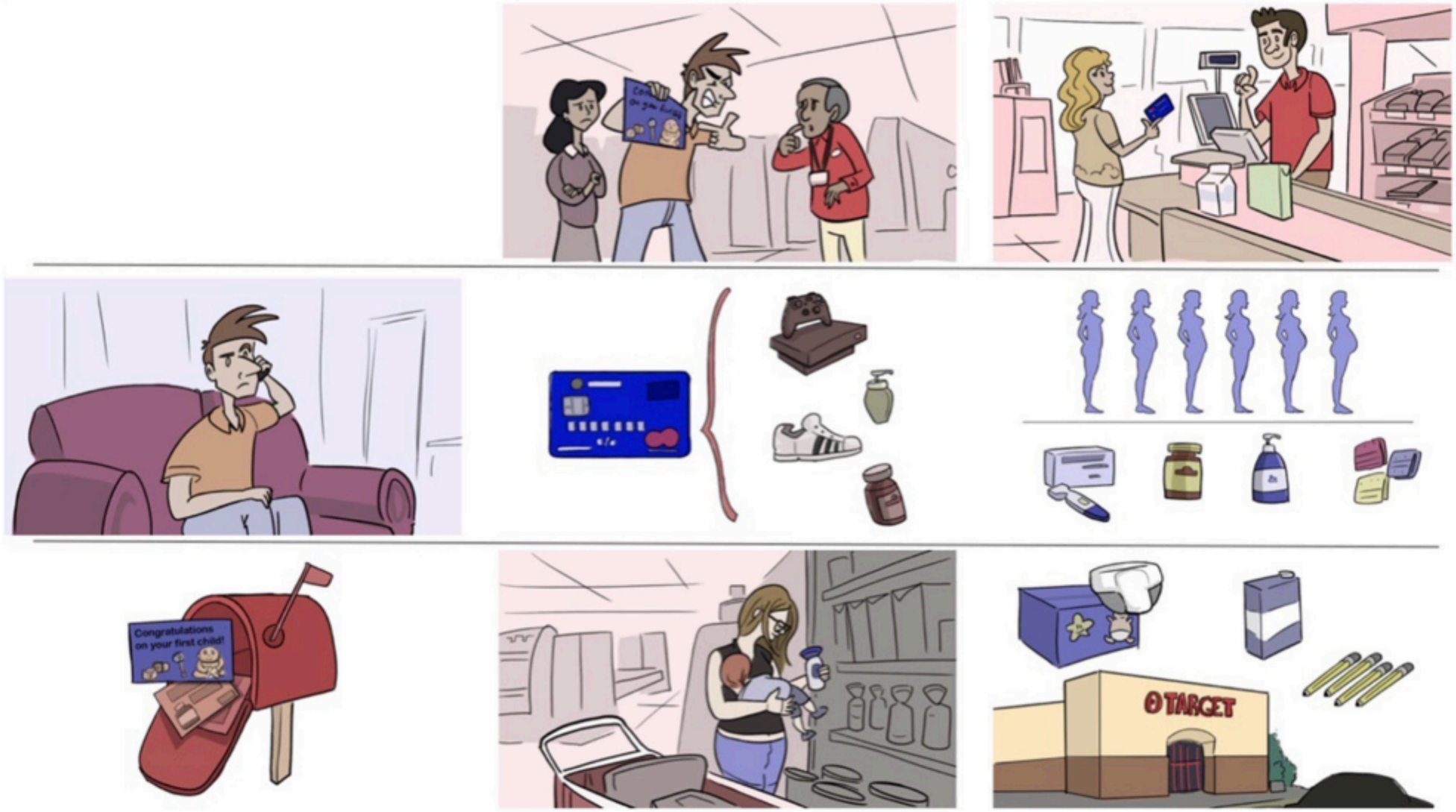
Postmortem

JOHN LUNNEY, SUE LUEDER, AND GARY O'CONNOR, GOOGLE | APRIL 24, 2018

Postmortem culture: how you can learn from failure

Failures are an inevitable part of innovation and can provide great data to make products, services, and organizations better. Google uses "postmortems" to capture and share the lessons of failure.

Which step is wrong?

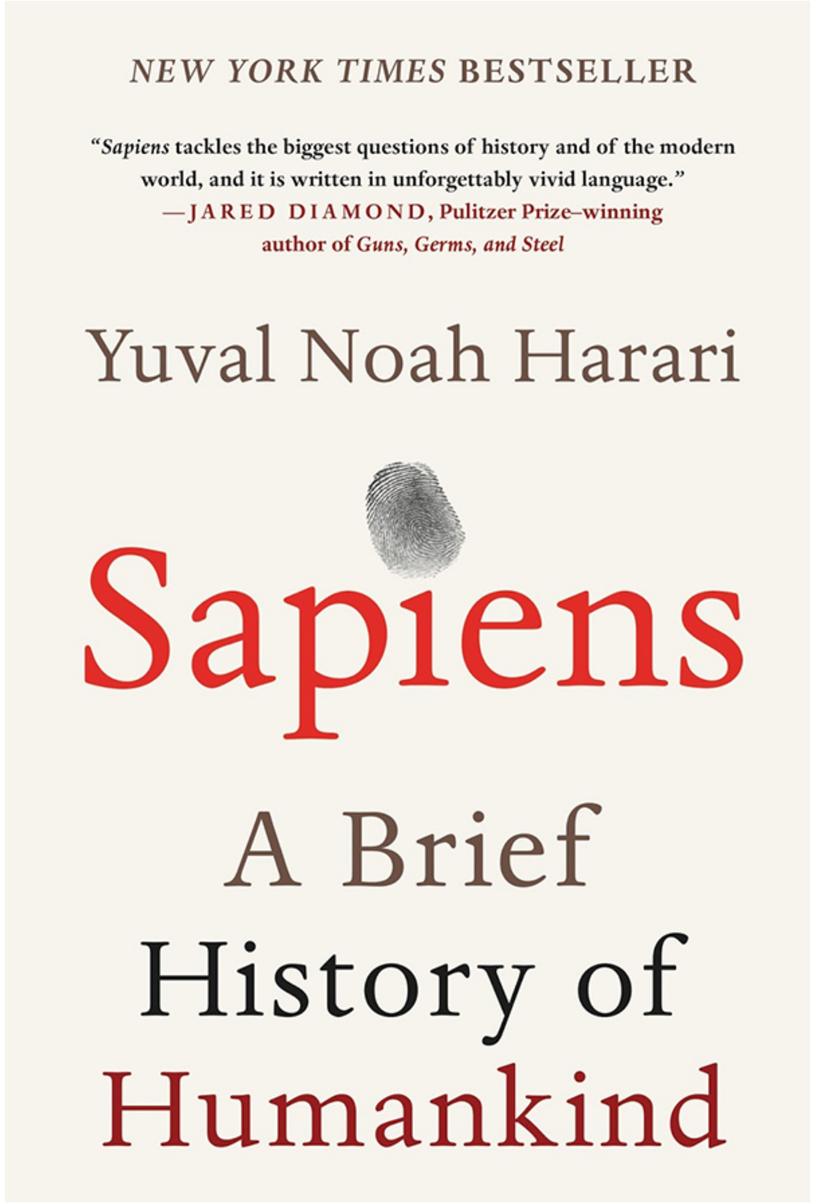


Technology is a double- edged sword. Its power - for good and for bad - resides in us, i.e. people (users) determine what they do with technology.

Technology design is political.

Traditional models

- Private vs. Public Places
- Private vs. Public Information



gossip played a crucial role in the evolution of Homo sapiens, enabling them to form large, complex societies through intricate social cooperation by allowing individuals to understand the social dynamics within their group, like who is trustworthy, who is cheating, and who can be relied upon, which was essential for survival and reproduction in large communities;

the need for privacy is a socially created need. Without society there would be no need for privacy.

Society is fraught with conflict and friction. Individuals, institutions, and governments can all engage in activities that have problematic effects on the lives of others.

Privacy is the relief from a range of kinds of social friction.

Why is traditional model insufficient?

Westin 1967. Privacy and control over information

"Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"

- Relevant when you give personal information to a web site; agree to privacy policy posted on web site
- May not apply to your personal health information

What are the limitations?

Fair Information Principles

- **Collection Limitation.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data quality principle.** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Fair Information Principles

- **Purpose specification.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use limitation principle.** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law.

Fair Information Principles

- **Security safeguards principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- **Openness principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.

Fair Information Principles

- **Individual participation principle.** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him

  - within a reasonable time;
  - at a charge, if any, that is not excessive;
  - in a reasonable manner; and
  - in a form that is readily intelligible to him;

(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

Fair Information Principles

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended.

- **Accountability principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Why is FIPS insufficient?

Puzzles

- Paradoxes:
  - say one thing, do another
  - New Media exhibitionism: Cams, blogs, etc.
- Cultural and historical differences

Goal of work

Justificatory framework: an analytic model (or theory) for reasoning through hard cases and puzzles.

Norms of Information Flow

- Norms of Appropriateness
  - Governing types/categories of information
- Norms of Transmission
  - Governing flow of information from agent to agent
    - Volunteered
    - Inferred
    - Mandated
    - Third party confidentiality
    - Commercial exchange
    - Reciprocal vs. one-way
    - Dessert
    - Etc.

Contextual Integrity

CI is preserved when norms of appropriateness and flow are respected; it is violated otherwise.

Application Heuristic

Detecting Change

A. What is the governing context?
B. What type of information?
C. According to what transmission principles (flow and actors)?

Red flag if CI is violated.

The Problem of Conservatism

- Opportunity Costs
- Tyranny of the Normal
  - e.g. Kyllo vs. United States (2001)
- Novel contexts: blogs? AIM?

Adjudicating Change

Normal practice may not be norm driven

Reform? When should norms be revised?

- Value/goals/ends of the context (e.g. healthcare)
- Moral and political considerations
  - Harm (e.g. stigma, discrimination, identity theft)
  - Justice, power, distribution of goods (tyranny?)
  - Freedom, autonomy, democracy, property

Revolution? When change threatens context

- Confidentiality in psychotherapy
- Anonymous voting in democratic elections

Contextual Integrity [Nissenbaum 2004]

- Philosophical framework for privacy
- Central concept: *Context*
  - Examples: Healthcare, banking, education
- What is a context?
  - *Set of interacting agents in roles*
    - Roles in healthcare: doctor, patient, …
  - *Informational norms*
    - Doctors should share patient health information as per the HIPAA rules
    - Norms have a specific structure (descriptive theory)
  - *Purpose*
    - Improve health
    - Some interactions should happen - patients should share personal health information with doctors

Informational Norms

"In a context, the flow of information of a certain type about a subject (acting in a particular capacity/role) from one actor (could be the subject) to another actor (in a particular capacity/role) is governed by a particular transmission principle."

Contextual Integrity [Nissenbaum2004]

Privacy Regulation Example (GLB Act)

Sender role — Subject role

Financial institutions must notify consumers if they share their non-public personal information with non-affiliated companies, *but the notification may occur either before or after the information sharing occurs*

Attribute — Recipient role — Transmission principle

Why is Contextual Integrity insufficient?

Approximate information flow

Principle of minimum asymmetry

Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing

Xiaodong Jiang, Jason I. Hong, and James A. Landay

Group for User Interface Research
Computer Science Division
University of California, Berkeley
Berkeley, CA 94720-1776, USA
{xdjiang, jasonh, landay@cs.berkeley.edu}

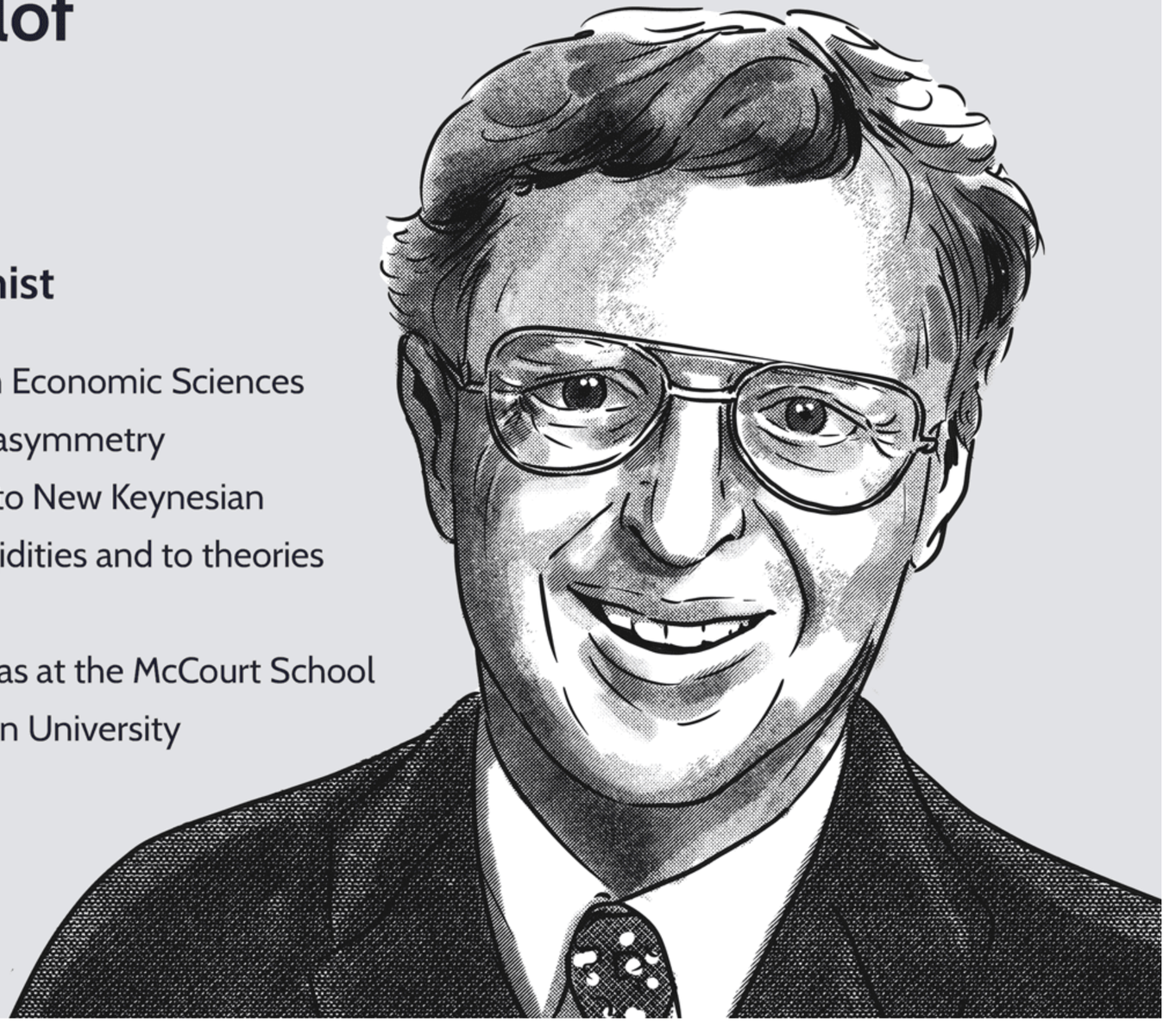
Abstract. In this paper, we propose a framework for supporting socially-compatible privacy objectives in ubiquitous computing settings. Drawing on social science research, we have developed a key objective called the *Principle of Minimum Asymmetry*, which seeks to minimize the imbalance between the people about whom data is being collected, and the systems and people that collect and use that data. We have also developed *Approximate Information Flow* (AIF), a model describing the interaction between the various actors and personal data. AIF effectively supports varying degrees of asymmetry for ubicomp systems, suggests new privacy protection mechanisms, and provides a foundation for inspecting privacy-friendliness of ubicomp systems.

George A. Akerlof

Born: June 17, 1940

New Keynesian Economist

- 2001 Nobel Prize Recipient in Economic Sciences for his theory of information asymmetry
- Has also made contributions to New Keynesian theories of price and wage rigidities and to theories of social economics
- Professor at Berkeley, as well as at the McCourt School of Public Policy at Georgetown University



Investopedia

THE MARKET FOR "LEMONS": QUALITY UNCERTAINTY AND THE MARKET MECHANISM *

GEORGE A. AKERLOF

I. INTRODUCTION

This paper relates quality and uncertainty. The existence of goods of many grades poses interesting and important problems for the theory of markets. On the one hand, the interaction of quality differences and uncertainty may explain important institutions of the labor market. On the other hand, this paper presents a struggling attempt to give structure to the statement: "Business in underdeveloped countries is difficult"; in particular, a structure is given for determining the economic costs of dishonesty. Additional applications of the theory include comments on the structure of money markets, on the notion of "insurability," on the liquidity of durables, and on brand-name goods.

There are many markets in which buyers use some market statistic to judge the quality of prospective purchases. In this case there is incentive for sellers to market poor quality merchandise, since the returns for good quality accrue mainly to the entire group whose statistic is affected rather than to the individual seller. As a result there tends to be a reduction in the average quality of goods and also in the size of the market. It should also be perceived that

Rejections and acceptance

By June of 1967 the paper was ready and I sent it to *The American Economic Review* for publication. I was spending the academic year 1967-68 in India. Fairly shortly into my stay there, I received my first rejection letter from *The American Economic Review.* The editor explained that the *Review* did not publish papers on subjects of such triviality. In a case, perhaps, of life reproducing art, no referee reports were included.

Michael Farrell, an editor of *The Review of Economic Studies,* had visited Berkeley in 1966-67, and had urged me to submit "Lemons" to *The Review,* but he had also been quite explicit in giving no guarantees. I submitted "Lemons" there, which was again rejected on the grounds that the *The Review* did not publish papers on topics of such triviality.

The next rejection was more interesting. I sent "Lemons" to the *Journal of Political Economy,* which sent me two referee reports, carefully argued as to why I was incorrect. After all, eggs of different grades were sorted and sold (I do not believe that this is just my memory confusing it with my original perception of the egg-grader model), as were other agricultural commodities. If this paper was correct, then no goods could be traded (an exaggeration of the claims of the paper). Besides – and this was the killer – if this paper was correct, economics would be different.

I may have despaired, but I did not give up. I sent the paper off to the *Quarterly Journal of Economics,* where it was accepted.

https://www.nobelprize.org/prizes/economic-sciences/2001/akerlof/article/

What is Privacy?

Privacy by policy vs. architecture

Privacy by Policy

- Through laws and policies
- Requires enforcement, tech can facilitate compliance
- Violations possible due to bad actors, mistakes, government mandates

Privacy by Architecture

- Through technology
- Reduces need to rely on trust & external enforcement
- Violations possible tech fails
- May be viewed as too expensive or restrictive