The Evolution of My View of HCI: Some Thoughts on HCI in Personalization and Privacy

John Karat
ACM SIGCHI
johnkarat@gmail.com
Themes in HCI

A primary goal that drew many to HCI was making technology for people that improves their lives.

How? Once upon a time (around 1980):
- Word processing was the “white rat” for psychologists in HCI.
- UIMS was a dominant theme for efficiently going from requirements to code (tools not rules).
- Usability and productivity were the keys.
This figure shows the results of cluster and multivariate analysis of the top 64 author cocitations in the HCI literature. Source: Wania, Atwood and McCain, DIS 2006. reprinted with permission.
But Things Have REALLY Changed

- Productivity (usability) issues largely reduced by consistency (we knew this would happen)

- But HCI did not say “problem resolved, let’s do something else”

- We have looked more broadly at what it means to design technology that is increasingly important in peoples lives.
How to Decide What is Important?

Hindsight is Easy But Still Illustrative

– We didn’t see “Google it” coming
– We didn’t understand that engagement trumps ease of use
– What will happen with 3-D printers?
– Human-Information Interaction, Communication, Augmented Cognition
– Today, we strive for much greater impact than we previously thought possible
My Story of a 10 Year Research Thread

From 2000 to 2010

- Moving through Cognitive modeling, Input mechanisms (pointing, touching, speaking), Medical Records, Collaboration tools …

Personalization (how might systems behave if they knew the user) was rising

- Research FUNDING at IBM was offered to “develop a deeper understanding”
- 2000 was not a year when you could turn down money
What Our Findings Showed About Personalization in eCommerce

- We asked what people thought personalization was.

- **Personalizing a user experience** means making use of personal data in a business context to provide *value* to the *customer* and the *business*.

- *Information* about a user can be either *explicitly* gathered or *implicitly* obtained through a variety of methods (e.g., data mining, recommender systems).

- For a user, **Personalization Value** builds on *privacy*, *security*, and *trust* in the context of the user task.
Privacy, Security, and Trust in the Personalization Context

Customer **Trust**: of an ebusiness develops through their perception that the data they provide is *secure*, will be used only as they *allow*, and provides them *value*.

**Privacy**: the control a user has over access to and use of their personal information.

**Security**: the confidence that data can not be compromised or taken by unauthorized sources.
Personalization Research Conclusions

Our research indicated that personalization should not be thought of as a single feature (we tested about 70), but rather as a space in which different features have different values depending on the user and business contexts.

Gave rise to a new set of questions that required much broader thinking than something like “fixing error correction in speech recognition systems”.
IBM decided personalizing its website really wasn’t central to its business
– It used the results, but they had limited impact
There was interest in the identification of privacy (sort of by accident) as a primary user concern
A new “customer” (CPO) asked for a “deeper understanding” project on privacy
What We Found About Privacy Policies from an IT Perspective

- Enterprises collect large amounts of personally-identifiable information (PII).
- Because of the potential for abuse, it is desirable that access to PII be restricted by policies.
- A privacy policy is a set of rules for how PII can be accessed and used by the enterprise.
- A privacy rule has up to 6 components: User categories, Actions, Data categories, Purpose, and [Conditions, Obligations].
- Organizations would like to be open about data use, but this is difficult to do with guarantees.
What IT Organizations Wanted - Bridging the Gap from Policy to Practice

- There is a **business need for usable policy management technologies** for individuals and organizations (e.g., OECD, HIPAA).

- **Policy** is a part of a variety of organizational processes.

- Policy as **understood by the people** can be different than the policy **defined in the IT systems**.

- For example, ensuring that intended and implemented policies are in sync is a substantial challenge.
For more than 150 years, our company has been a trusted symbol of service and reliability. We safeguard your customer information carefully….

Structured rules
Billing representatives can use customer address for the purpose of mailing invoices

Implementation
Mary Q. Employee is allowed READ access to database record #729 at 12:37pm on August 12
How SPARCLE Parses Policy Rules

Marketing employees

User category

*can* collect and use

Actions

name, address, and phone number

Data categories

*for the purpose of* direct advertising

Purpose

*if* the customer has opted-in.

Condition

- Unconstrained authoring yielded low quality
- Natural Language (NL) and Structured Entry yielded good quality
- Including both methods seems to be most promising direction
A Lot of Enthusiasm, But …

Consider the ACLU Pizza video, or the recent book “The Circle”

We were really saying that data needs to be “policy aware”, but …

– Where was the force to drive the required developments to support this

– This seemed to be a call for greater involvement of HCI in policy
Is HCI Really Up to the Task?

How to we argue for a more prominent role?

– Do we really believe in this?
  - What is our training?
  - What are our skills?
  - Should we be focused on influencing policy makers?
  - Maybe Jan will help us out here (later today)

This is different from working on usability or software engineering
Some Subtle Considerations

Has HCI training kept up with this broadening in focus, or does it need to change?

– Who cares more about augmenting human capabilities – CS or Behavioral Science?
– How much is going from Requirements to Code (which I would argue is the CS focus) missing the point (HCI should be more concerned with setting requirements important to humans)
Some Concluding Comments

- Personalization work led to privacy and security policy research, development, and product.

- Our focus on NL authoring led to partnering with research teams developing NL tools – including tools that went into Watson.

- Our usable security work led to university partnerships and government contracts.
Thank you