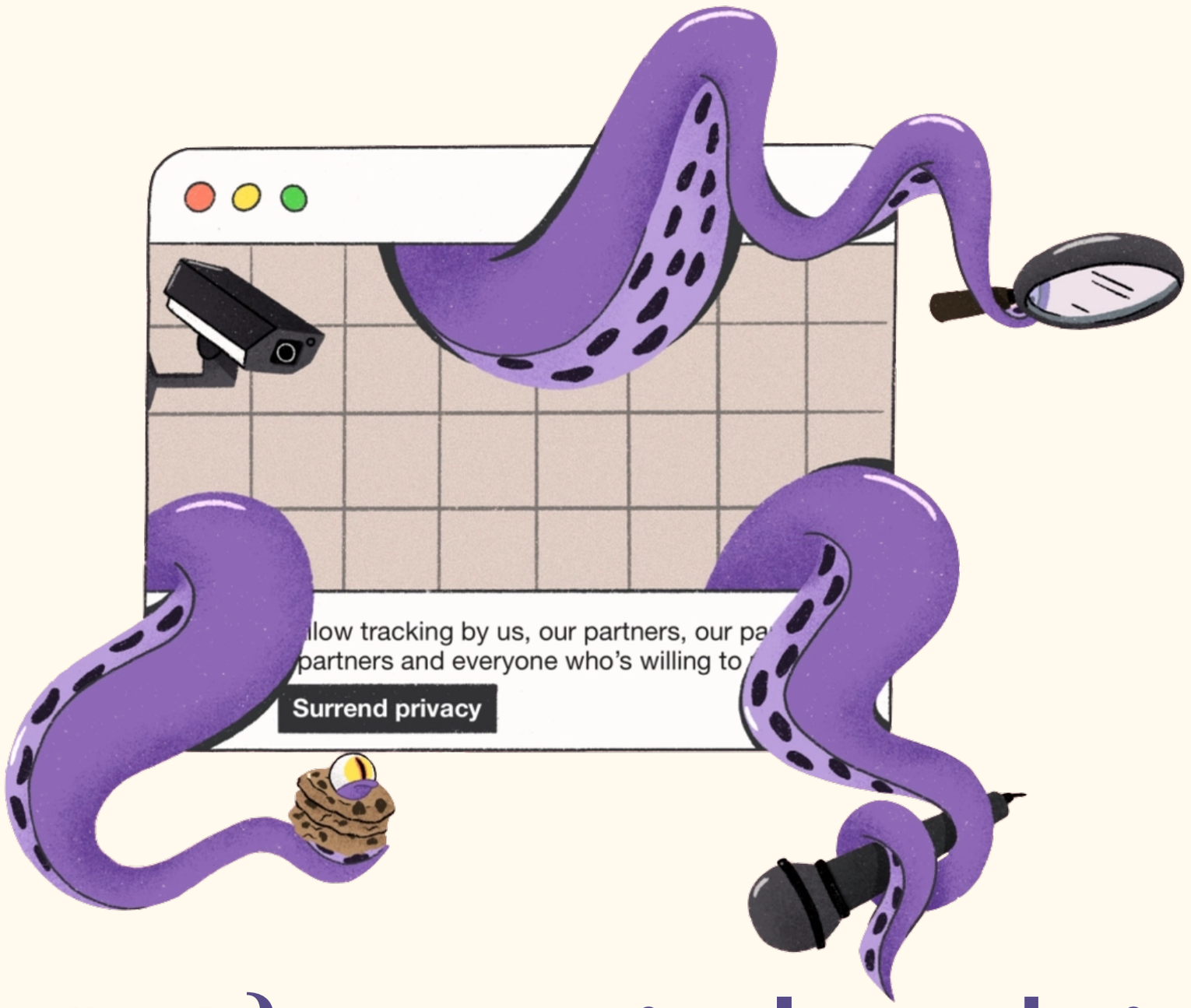


Ex{CS}tential Ethics

an Independent Project, by Claire & Olha with Dr. Bhardwaj

MYTHS.

FOUR DANGEROUS MYTHS ABOUT PRIVACY

1. Privacy is about hiding dark secrets & those with nothing to hide have nothing to fear
2. Privacy is about concealing creepy things that other people do with your data
3. Privacy means being able to control how your data is used
4. Privacy is dying

MYTHS.

FOUR DANGEROUS MYTHS ABOUT PRIVACY

1. **Privacy is about hiding dark secrets & those with nothing to hide have nothing to fear**
2. Privacy is about concealing creepy things that other people do with your data
3. Privacy means being able to control how your data is used
4. Privacy is dying

"If you have nothing to hide, you have nothing to fear."

People have historically used "nothing to hide" — novelists like Richard James or Nazi leaders like Joseph Goebbels, and was used to justify numerous state surveillance programs in democracies like the UK & the US.

It's *wrong on its own term*, because everyone has something he need to keep private as part of a basic human need.

MYTHS.

FOUR DANGEROUS MYTHS ABOUT PRIVACY

1. Privacy is about hiding dark secrets & those with nothing to hide have nothing to fear
2. **Privacy is about concealing creepy things that other people do with your data**
3. Privacy means being able to control how your data is used
4. Privacy is dying

Creepiness is the most common reaction people experience when they learn about a new privacy theory or invasive information practice. Things like *surveillance-based advertising*, *Facebook's experiments to control user emotions*, *NSA surveillance*, *eavesdropping "smart" Barbie dolls...*

Creepiness (if used as a policy for privacy) is both overinclusive & underincusive. It also relies on human emotional responses, which is social constructed and easily manipulated. A good example of Target.

MYTHS.

FOUR DANGEROUS MYTHS ABOUT PRIVACY

1. Privacy is about hiding dark secrets & those with nothing to hide have nothing to fear
2. Privacy is about concealing creepy things that other people do with your data
3. **Privacy means being able to control how your data is used**
4. Privacy is dying

Privacy isn't actually primarily about control, even if it runs deep in our legal & cultural understanding of it. Famous articles and papers on privacy had framed it as a way to determine for themselves how & to what extent information is shared with others. Tech companies give you this illusion with privacy dashboards & settings.

It's been a massive *failure*. Control is overwhelming, an illusion, completes the creepy trap, and is insufficient. **Design** choices are made where uses have an illusion of choice

MYTHS.

FOUR DANGEROUS MYTHS ABOUT PRIVACY

1. Privacy is about hiding dark secrets & those with nothing to hide have nothing to fear
2. Privacy is about concealing creepy things that other people do with your data
3. Privacy means being able to control how your data is used

4. Privacy is dying

Tech companies *love* to tell you that privacy is dying. Hint: it's not! They like to say that because it works in their favor.

There's a grain of truth: the amount of human information being collected is increasing. But the claim itself takes this fact & adds the empirical claim that *people don't care about privacy* and the moral claim that *it's okay to not worry about privacy*. Both of this are fundamentally incorrect.

People claim that young people don't care—we grew up in a time of social media. This is wrong: young people have more sophisticated needs for privacy than the elderly.

(we're focusing mainly on informational privacy)

So... what is privacy?

Informational Privacy — measure of access to which information about humans is used as well as known through information, attention, and physical proximity.

This presentation will be about why privacy matters, how we can enforce privacy, and how to resolve contradictions within such regulation.

Other "Privacies" we don't discuss today but it intersects closely with these:

- Spatial Privacy — "Right To Be Alone"
- Decisional Privacy — i.e. right for abortions

Imagine life in a fishbowl, where people are visible from a single point. What risks does that pose?

1) **Extrinsic losses of freedom** — people curtail outward behaviors that might be unpopular, unusual, unconventional.

2) **Internal losses of freedom** — arise from internal censorship caused by awareness that one's every action is being noted and recorded.

3) **Political implications?** Everyone adhering to the safe "norm"!

Privacy is important because it protects the diversity of personal choices and actions, not because it protects the freedom to harm others and commit crimes.

Privacy also prevents:

- **Informational Harm** — ranges from physical to reputitional

  example— case of murder of actress Rebecca Schaeffeer whose address was gleaned from then freely available drivers' records

- **Informational Inequality** — benefits from information collection benefit disproportionately to corporate and governmental actors.

- **Informational Injustice** — happens when information from one sphere *(religious affiliation, medical history)* migrates to other *(files of company considering an individual for employment)*

Privacy is important because it promotes our values such as democracy, ability to shape and express our personalities (authenticity), safety. Extent of privacy influences how whether our values are fulfilled.

Three Principles governing privacy legislation:

1. Protecting privacy of individuals against intrusive government agents
2. Restricting access to intimate, sensitive, or confidential information
3. Curtailing intrusions into spaces or spheres deemed private or personal

1. Protecting privacy of individuals against intrusive government agents

Amendments referenced:
1 — speech, religion, association
3 — quartering soldiers
4 — search and seizure
5 — self-incrimination
9 — general liberties
14 — personal liberty vs. state action

Privacy must be protected by well-defined and generally accepted political principles.

In the US, the Constitution & the Bill of Rights act as limits on what the government can do. The 1st, 3rd, 4th, 5th, 9th, and 14th amendments combined create a law of privacy.

The **Privacy Act of 1974** placed significant limits what the agencies of federal government could use the databases of personal information for. George Orwell's *1984* book sparked the public's imagination and therefore the Code of Fair Information Practices was formed.

2. Restricting access to intimate, sensitive, or confidential information

This focuses on the *nature* of the information collected/disseminated.

Defining **sensitive information:**

- Family Educational Rights & Privacy Act of **1974**
- Right to Financial Privacy Act of **1978**
- Video Privacy Protection Act of **1988**
- HIPAA of **1996**

The common law recognizes a breach of privacy as a harm: "public disclosure of embarrassing private facts about the plaintiff" or an "intrusion into the plaintiff's privacy affairs."

3. Curtailing intrusions into spaces or spheres deemed private or personal

There is a belief in the "protected private zone" in the 3rd & 4th amendments that define explicit limits on government access to a home. There are a few Supreme Court rulings that expand this to a "digital" home—*Katz vs. US* and *California vs. Greenwood*.

Example: “California v. Greenwood”

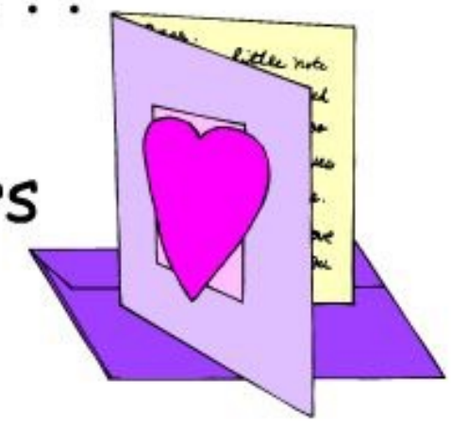
- Case heard by the US Supreme Court in 1988.
- Billy Greenwood was arrested as suspected drug dealer.
- The police collected most of the evidence against Greenwood from dark trash plastic bags. Police conducted the search without warrant.
- Greenwood argued that the search violated his Fourth Amendment right against unreasonable searches and seizures.
- The Supreme Court ultimately ruled in favor of the police, stating that individuals do not have a reasonable expectation of privacy in the trash they leave outside their homes because trash is "in the public space"
- Shows a focus on **location** — whether inside or outside what is conserved a person’s private sphere.

Think about this question:

Are there things you throw away that you and your family would not like everyone to see?

How about . . .

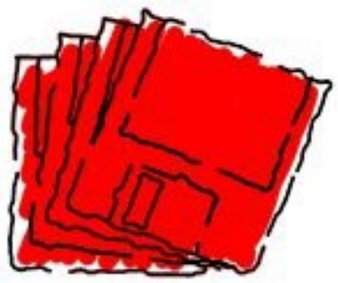
Love letters



Receipts

Notes home from teachers

Computer disks



Underwear

Photos

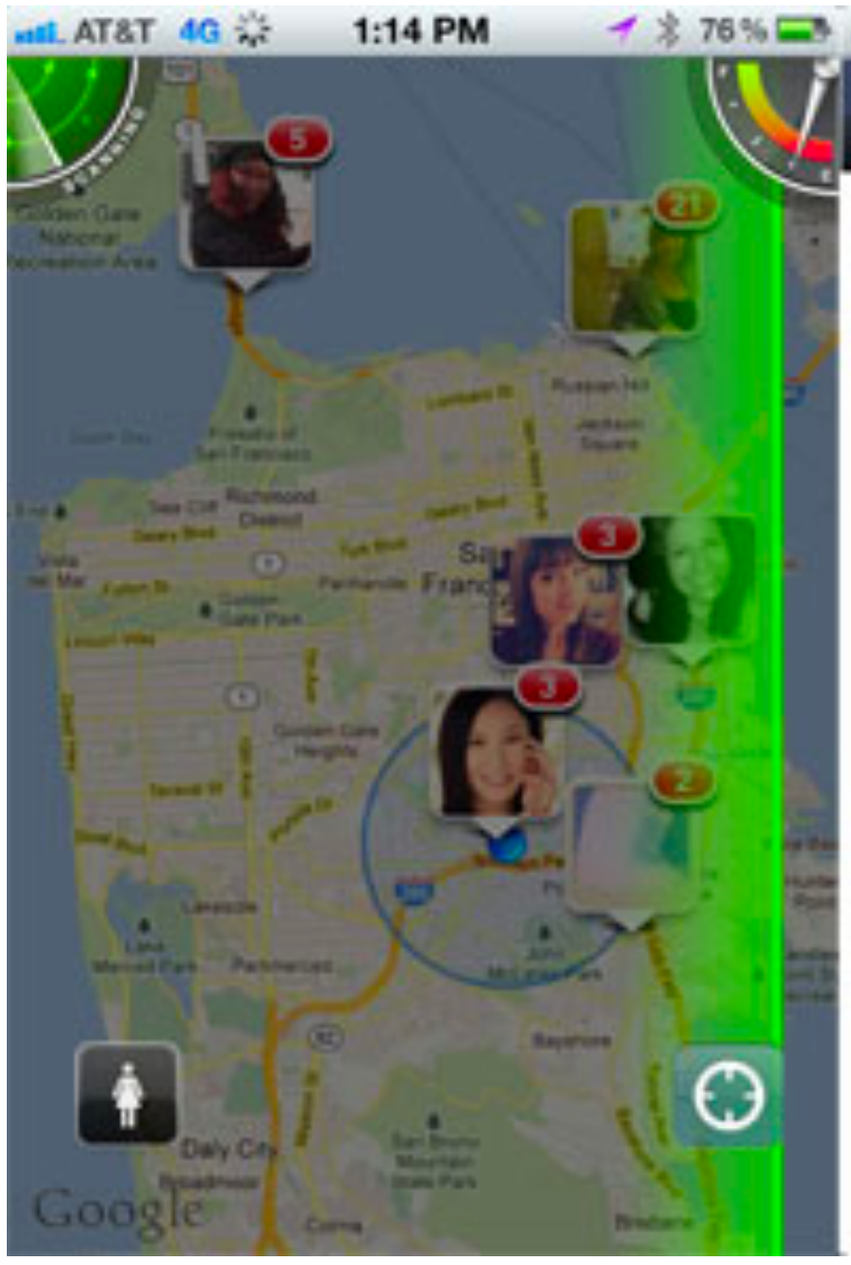
Three Principles

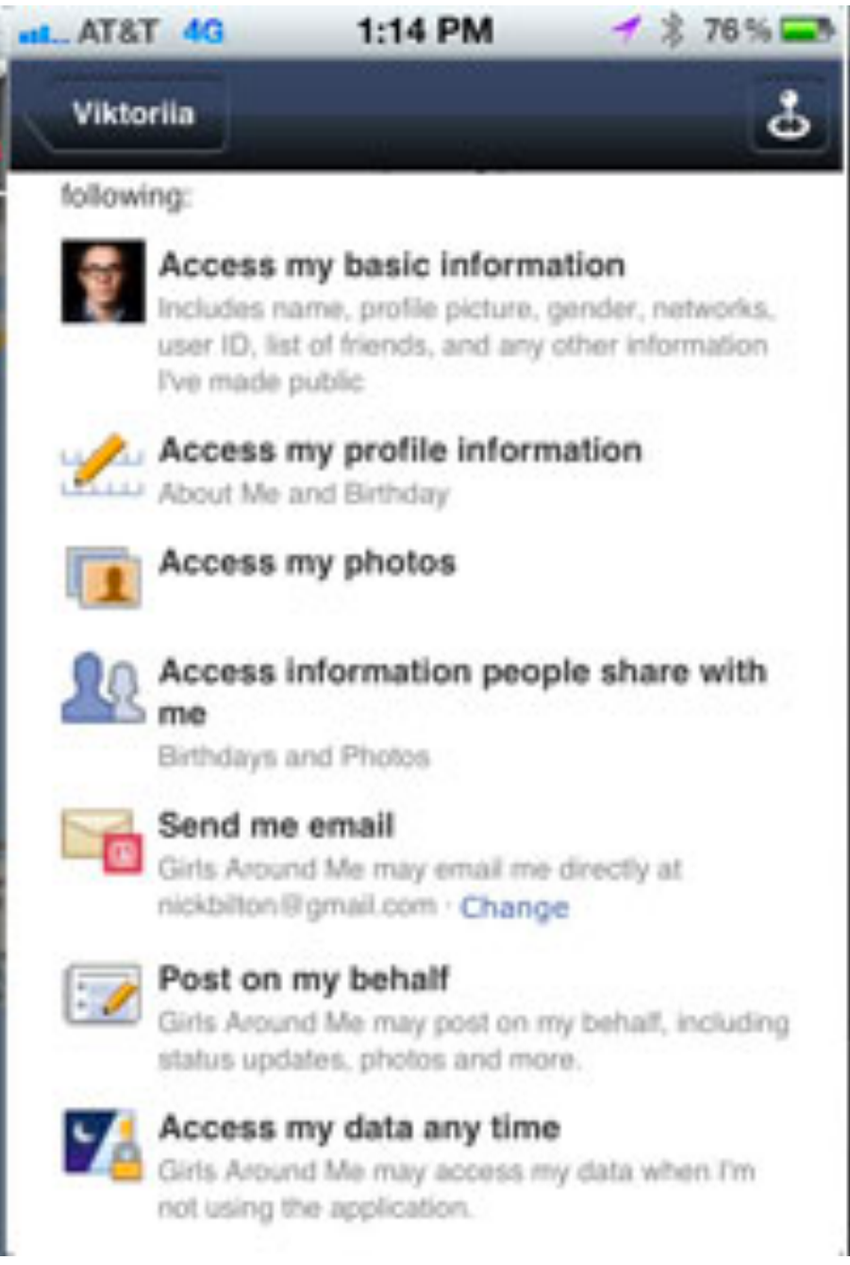
1. Protecting privacy of individuals against intrusive government agents
2. Restricting access to intimate, sensitive, or confidential information
3. Curtailing intrusions into spaces or spheres deemed private or personal

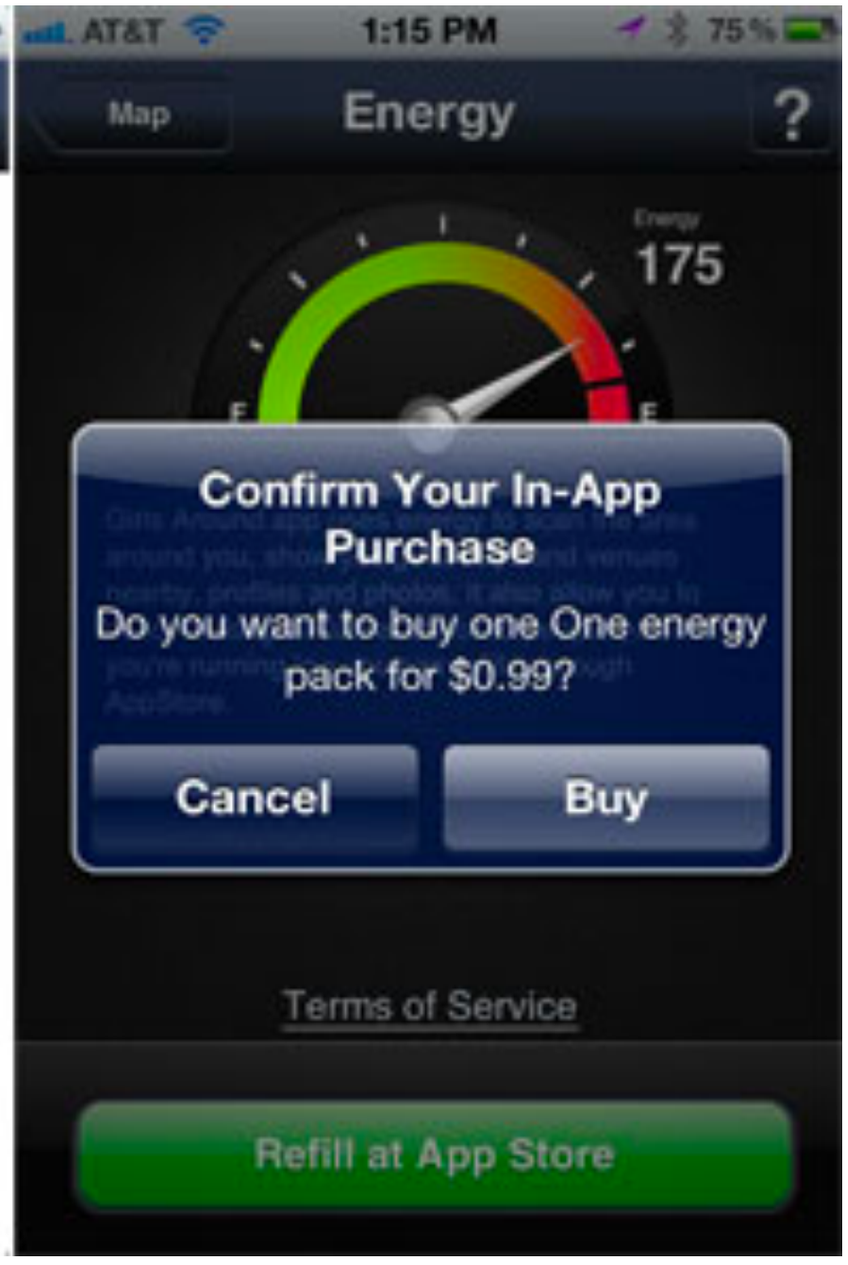
Legislation appears to be operating on dichotomies— government agents and private individuals, sensitive and non-sensitive, private and public”

BUT, IS IT ENOUGH? We have already seen some challenges & gray areas in previous examples, but let's dive deeper.

“girls around me” app







“it was not illegal, it was distasteful” **(2012)**

Home / Business / Developer

Stalker app Girls Around Me hunts women via Faceboo

Online outrage increases over sexualized, s stalking app Girls Around Me - though it is first of its kind.

Media & Entertainment

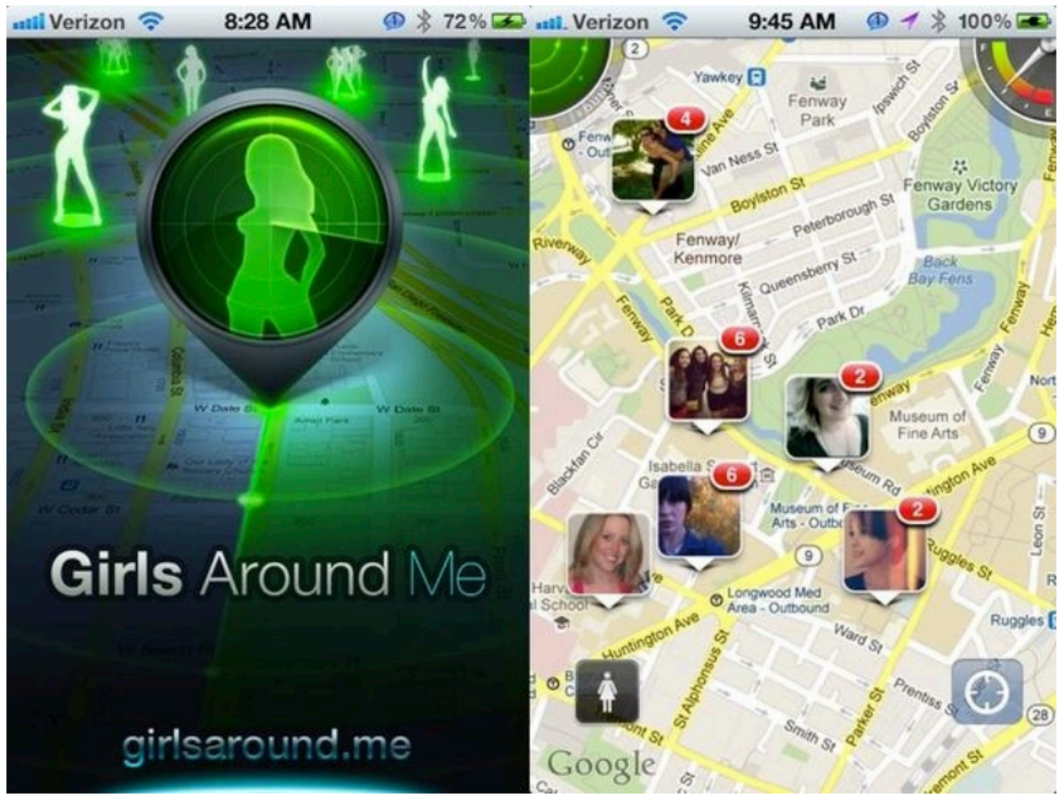
"Girls Around Me" Creeper App Just Might Get People To Pay Attention To Privacy Settings

Devin Coldewey @techcrunch / 6:30 PM EDT • March 30, 2012

Comment

Location Information

- [x] Include me in the public list of people who are currently checked in at a venue ?
- [x] Let me earn Mayorships (I realize that Mayorship is a public office) ?
- [x] When my friends check in with me, it's okay to include my name on their check-in tweets or Facebook wall posts ?
- [x] Let venue managers see when I check in to their business, or when I am one of their best customers ?



Many of the people being tracked by this app, male and female, haven't even considered the idea that their movements might be tracked systematically by a stranger.

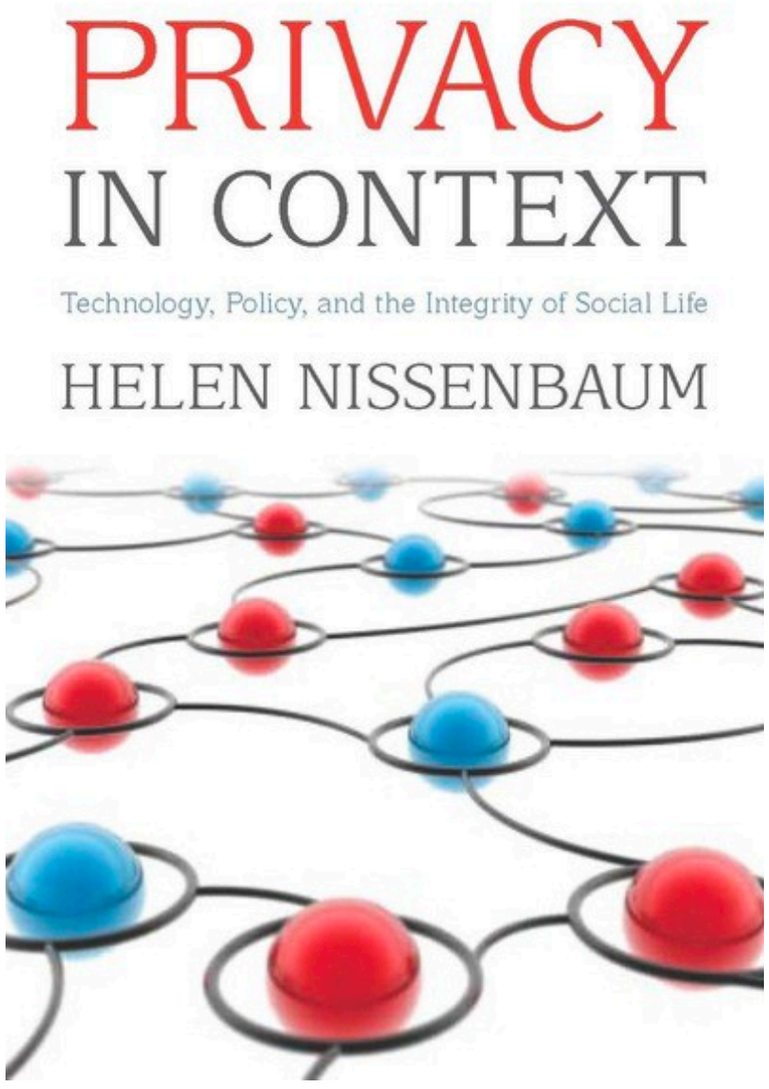
Ambient Social Apps

3 principles on which current legislation about privacy don't work anymore:

Users consented (voluntarily provided to facebook as part of social expectations) to their location data being public. The **CONTEXT**, however, made it feel as an intrusion of privacy

This leads us to the **Contextual Integrity** approach to privacy.

In an *Atlantic* article about the app Girls Around You, a reporter cites contextual integrity (pioneered by Nissenbaum).



Practices/norms can be evaluated in terms of:

- Effects on the interests and preferences of affected parties
- How well they sustain ethical and political (societal) principles and values
- How well they promote contextual functions, purposes, and values

5 parameters for considering context:

1. the data subject
2. sender of the data
3. recipient of the data
4. information type
5. transmission principle

- considers events in a context not only of place but of politics, convention, practices and cultural expectation
- information should not cross contexts: information revealed in a particular context is **always tagged with that context** and never “up for grabs"
- informational norms should be internal to a given context — **norms are relative**

Implications of contextual integrity:

There are no elements of life that aren't governed by the *norms of informational flow*—everything happened within a sphere of cultural, political, or conventional expectations. Each sphere has its own distinct set of norms.

Norms of appropriateness dictate what information about persons is fitting to reveal in that **specific** context. In a way, this can be summed into "none of your business."

Distributive justice in the context of data: data can be a social currency each with a defined social good.

When privacy is considered in these contextual spheres, information should bever be "up for grabs" & we must remember that norms are non-universal.

Important Context to Consider on Example of Facebook's "Real Name Policy"

- Facebook "Real Name Policy" — under which customers are required to use their real names rather than pseudonyms.

- "Having two identities for yourself" Zuckerberg argues for clear example of "integrity."

- Note: Behind the scenes, Real Name Policy is undeniably good for facebook enhancing both power and profitability

- How did this policy impact people?
    - Native and indigenous Americans with surnames like Creeping Bear get their accounts suspended
    - Members of the trans and drag communities were forced into binary-gendered identities
    - Political activists in authoritarian states get persecuted for their social media posts

LACK OF PRIVACY MOSTLY IMPACTS ALREADY OPPRESSED MINORITIES

Design Principles

Norms and architecture are shaped by engineers using the power of data & behavioral science. The **design** of interfaces with with *limited choices* allows controlling behavior and gives users the illusion of transparency.

- Example of Facebook & their privacy settings
- Capitalizing on people's lack of knowledge & time
- We see that “putting users in control through notice and choice” is actually controlling users through overwhelming and manipulative scheme of privacy self-management
- Like to blame users for failing to do the privacy work (i.e., blaming younger generations for being too public online rather than enforcing privacy rules.)

Design Principles - enacting real change:

Using principles of good design to help enforce contextual integrity into privacy laws & norms:

1. View change as emergent from an accountable & collaborative *process*
2. *We share the design knowledge & tools & work with communities (keep it transparent and easily access!)*
3. An understanding that everyone is an "expert" based on their own lived experiences and different people are affected differently by privacy regulations
4. Work towards non-exploitative solutions that consider the intricacies of different privacy spheres
5. Before seeing new solutions, we look at examples of what have and have not worked.

REFERENCES & FURTHER READING

Privacy as Contextual Integrity, by Helen Nissenbaum https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

Unpopular Privacy, by Anita Allen https://www.amazon.com/Unpopular-Privacy-Studies-Feminist-Philosophy/dp/0195141377

A Theory of Creepy: Technology, Privacy, and Shifting Social Norms, by Tene & Polonetsky https://yjolt.org/theory-creepy-technology-privacy-and-shifting-social-norms

Design Justice, by Sasha Constanza-Chock https://designjustice.mitpress.mit.edu/

The Design of Everyday Things, by Don Norman https://www.goodreads.com/book/show/840.The_Design_of_Everyday_Things

https://bit.ly/excstential-readings


THANK YOU
THANK YOU
THANK YOU
THANK YOU
THANK YOU
THANK YOU
THANK YOU