

# Lecture 3: Privacy

CMSC 25910

Spring 2022

The University of Chicago



THE UNIVERSITY OF  
CHICAGO

# Privacy Hot Takes

## Facebook's Zuckerberg Says The Age of Privacy Is Over

By MARSHALL KIRKPATRICK of  **ReadWriteWeb**  
Published: January 10, 2010

 PRINT

Facebook founder Mark Zuckerberg told a live audience yesterday that if he were to create Facebook again today, user information would by default be public, not private as it was for years until the company changed dramatically in December.

<https://archive.nytimes.com/www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html>

# Privacy Hot Takes



The image is a screenshot of a Forbes article. At the top, the word "Forbes" is written in white on a black background. Below that, the word "LEADERSHIP" is written in small, grey, all-caps letters. The main title of the article is "Privacy Is Completely And Utterly Dead, And We Killed It" in a large, bold, black font. Below the title, the author's name "Jacob Morgan" is followed by "Contributor" and a small circular icon. Underneath the author's name is a short bio: "I write about and explore the future of work!". To the right of the bio is a blue button with the word "Follow" in white. Below the bio and button, the date and time "Aug 19, 2014, 12:04am EDT" are displayed in a small, grey font. The main body of the article begins with the text: "Privacy...everyone keeps talking about it and apparently everyone is concerned with it, but going forward does it even matter? I recently watched the documentary, 'Terms and Conditions may Apply,' which provides a fascinating look at how organizations such as Facebook, Google, Apple, and others have changed the way they look at and approach privacy. After watching the movie it had me wondering, 'does privacy even matter anymore?'"

<https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/>

# Privacy Hot Takes

“You have zero privacy anyway. Get over it.”

Scott McNealy, Former CEO of Sun Microsystems (1999)

<https://www.wired.com/1999/01/sun-on-privacy-get-over-it/>

# Privacy Hot Takes

“If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time... that information could be made available to the authorities.”

Eric Schmidt, Former CEO of Google (2009)

[https://www.pcworld.com/article/515472/googles\\_schmidt\\_roasted\\_for\\_privacy\\_comments.html](https://www.pcworld.com/article/515472/googles_schmidt_roasted_for_privacy_comments.html)

# Privacy

“Some might say ‘I don't care if they violate my privacy; I've got nothing to hide.’ Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they ‘need’ a right: the burden of justification falls on the one seeking to infringe upon the right.”

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”

Edward Snowden, Whistleblower (2015)

[https://www.reddit.com/r/IAmA/comments/36ru89/just\\_days\\_left\\_to\\_kill\\_mass\\_surveillance\\_under/crqlgh2/](https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crqlgh2/)

# Privacy is Hard to Define

“Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”

Robert C. Post, Three Concepts of Privacy,  
89 Geo. L.J. 2087 (2001).

# Michael Wolf- The Transparent City





# Michael Wolf- The Transparent City



“Chicago has recently undergone a surge of new construction...In early 2007, the Museum of Contemporary Photography...invited Michael Wolf as an artist-in-residence....Wolf chose to photograph the central downtown area, focusing on issues of voyeurism and the contemporary urban landscape....his details are fragments of life—digitally distorted and hyper-enlarged—snatched surreptitiously via telephoto lenses

<http://aperture.org/shop/the-transparent-city/>

# Michael Wolf- The Transparent City



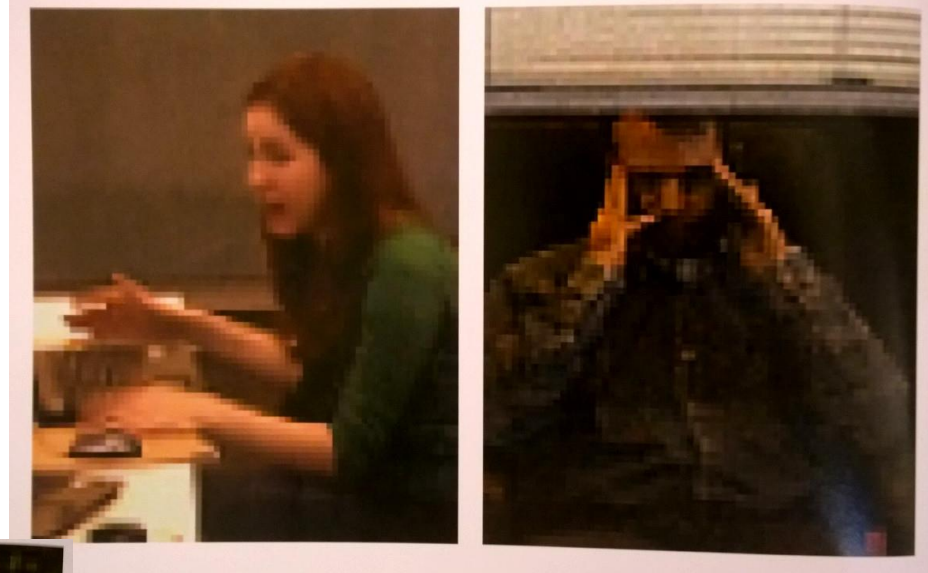
# Michael Wolf- The Transparent City



# Michael Wolf- The Transparent City

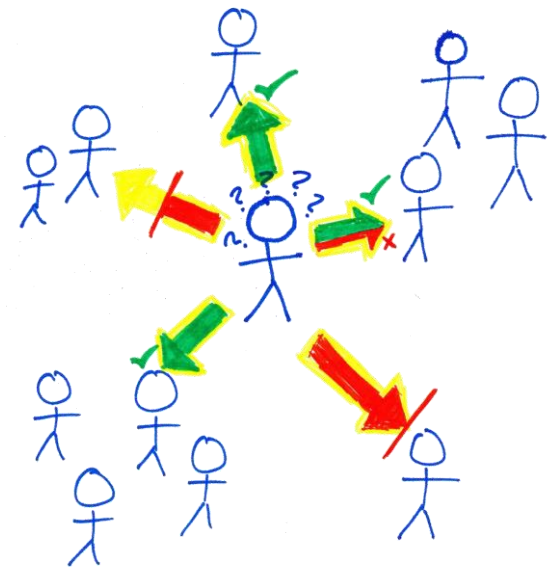


# Michael Wolf- The Transparent City





# Conceptualizing Privacy



# Warren and Brandeis (1890)



HARVARD  
LAW REVIEW.

---

VOL. IV.                      DECEMBER 15, 1890.                      NO. 5.

---

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."  
WILLES, J., in *Millar v. Taylor*, 4 Burr. 2303, 2312.

**T**HAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

# Warren and Brandeis's Inspiration



“Have you seen the Kodak fiend? Well, he has seen you. He caught your expression yesterday while you were recently talking at the Post Office. He has taken you at a disadvantage and transfixed your uncouth position and passed it on to be laughed at by friend and foe alike. His click is heard on every hand. He is merciless and omnipresent.”

The *Hawaiian Gazette*, 1890

<https://wirewheel.io/privacy-is-dead/>



# Warren and Brandeis's Argument

- “The individual shall have full protection in person and in property”
- The legal basis for fear
  - Battery → assault
  - Tangible property → intangible property
- Gossip pages about high society

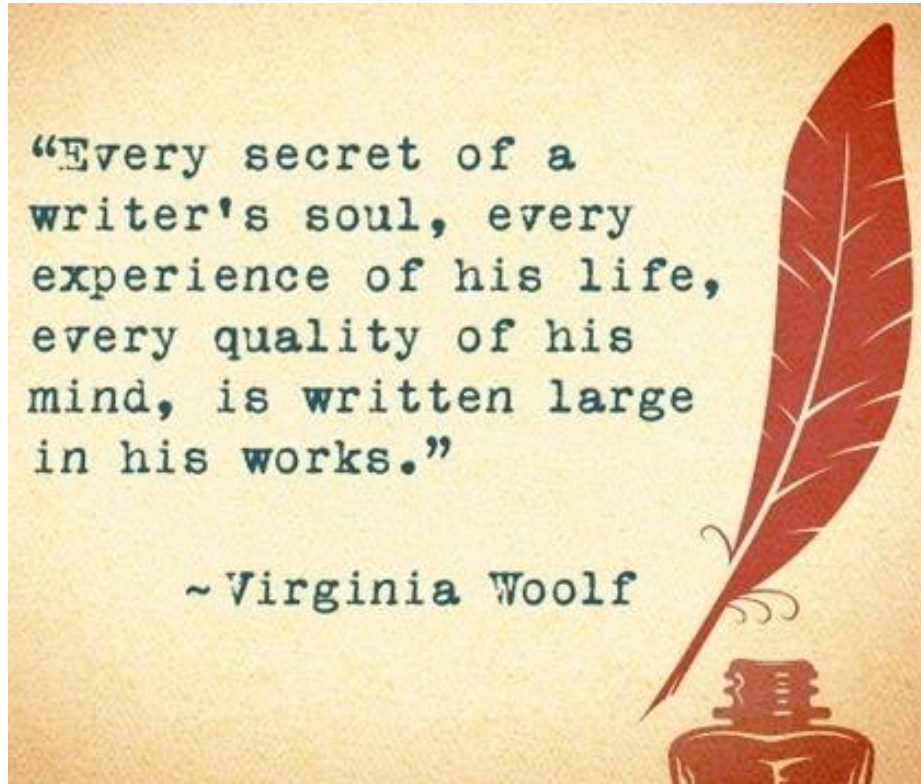
# Warren and Brandeis's Argument

- Libel and slander are insufficient in considering only damage to reputation
- Considers property rights
- The right to prevent, rather than profit from, publication
- **“The right to be let alone”**
- Excludes topics of general interest

# Photography Laws

Consent required for action related to a picture of a person in a public place (by country)			
Country	Take a picture	Publish a picture	Commercially <sup>1</sup> use a published picture
<a href="#">Afghanistan</a>	No	Yes (with exceptions)	Yes (with exceptions)
<a href="#">Argentina</a>	No	Yes (with exceptions)	Yes (with exceptions)
<a href="#">Australia</a>	No (with exceptions)	No (with exceptions)	Yes
<a href="#">Austria</a>	No	No (with exceptions)	Yes
<a href="#">Belgium</a>	No	Yes (with exceptions)	Yes
<a href="#">Brazil</a>	Yes	Yes	Yes
<a href="#">Bulgaria</a>	No	No	Yes
<a href="#">Canada</a>	Depends on province	Yes (with exceptions)	Yes
<a href="#">China</a>	No	No	Yes
<a href="#">Czech Republic</a>	Yes (with exceptions)	Yes (with exceptions)	Yes (with exceptions)
<a href="#">Denmark</a>	No	Yes (with exceptions)	Yes (with exceptions)
<a href="#">Ethiopia</a>	No	Yes (with exceptions)	Yes
<a href="#">Finland</a>	No	Yes (with exceptions)	Yes (with exceptions)
<a href="#">France</a>	Yes (with exceptions)	Yes (with exceptions) <sup>[3]</sup>	Yes
<a href="#">Germany</a>	No (with exceptions)	Yes (with exceptions)	Yes (with exceptions)
<a href="#">Greece</a>	No	No	Yes (with exceptions)
<a href="#">Hong Kong</a>	Depends on circumstances	Depends on circumstances	Depends on circumstances
<a href="#">Hungary</a>	Yes (with exceptions)	Yes (with exceptions)	Yes (with exceptions)
<a href="#">United Kingdom</a>	Depends on circumstances	Depends on circumstances	Depends on circumstances
<a href="#">United States</a>	No	No	Usually (although laws differ by state)

# Is Being “Let Alone” Sufficient?

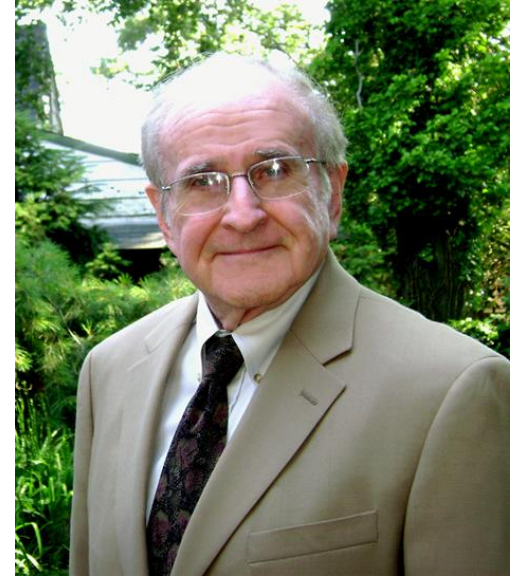


# Privacy as Control / Secrecy (1967)

“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.”

“...each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication....”

Alan Westin, *Privacy and Freedom*, 1967



# Is Limiting Access Sufficient?

- Individuals sometimes prefer to be let alone, yet sometimes want to be social
  - Privacy was traditionally “social withdrawal”

# Privacy Regulation Theory (1975)

- Irwin Altman (social psychology)
  - Preceded by Altman and Taylor's Social Penetration Theory (1973) about intimacy in relationships
- Dialectic and dynamic process of boundary regulation
  - Continuous movement on a continuum
- Goal: optimum balance of privacy and social interaction



# CPM Theory (1991)

- Sandra Petronio (communications)
  - Communication Privacy Management Theory
- Regulate boundaries based on perceived costs and benefits
  - Movement on a continuum
- Expect rule-based management
- Boundary turbulence related to clashing expectations





# Purpose Matters



# Purpose Matters

The Washington Post

Local

## Patients trusted Johns Hopkins gynecologist who allegedly videotaped them

By **Brigid Schulte** and **Peter Hermann** February 19, 2013 [✉ Email the author](#)

For more than two decades, women came to see Johns Hopkins gynecologist Nikita Levy and trusted him with not only the most private parts of their bodies but also with their innermost secrets. Listening to problems with husbands and boyfriends, the joys and frustrations of motherhood, Levy was a caring confidant, said patients and co-workers.

On Tuesday, they were reeling from [the news](#) that their doctor had committed suicide after being accused of surreptitiously videotaping and photographing many of his patients. Police said they have removed nearly 10 image-filled computer hard drives from Levy's home in Towson, Md.

# (Details)

- “For 25 years, Dr. Nikita Levy ran an obstetrics and gynecology practice out of the East Baltimore Medical Center, a community clinic run by the Johns Hopkins Hospital and Health System. Last February, Johns Hopkins authorities discovered that Levy had been secretly filming his patients in the examination room, using cameras embedded into pens that he wore around his neck and key fobs he carried in his pockets. At his home, police found hard drives and servers stocked with thousands of videos and photographs of his patient’s naked bodies, snapped under the auspices of performing routine pelvic examinations.”

# Privacy as Contextual Integrity (2004)

- Helen Nissenbaum (philosophy)
- “Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context.”

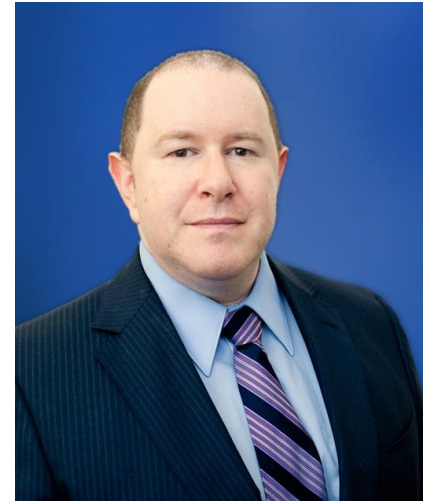


# Privacy as Contextual Integrity (2004)

- Appropriate flows of information
- Appropriate flows conform to contextual information norms
- Norms refer to the data subject, sender, recipient, information type, and transmission principle
- Conceptions of privacy evolve over time and are grounded in ethics

# Dan Solove's Pluralistic Conceptions

- Some data isn't "sensitive," but its collection and use impact privacy
  - Impact power relationships
  - Kafka-esque
- Solove's privacy taxonomy
  - Information collection
  - Information processing
  - Information dissemination
  - Invasion



# **Privacy Law and Regulation**

# How Privacy is Protected

- Laws, self regulation, technology
  - Notice and access
  - Control over collection, use, deletion, sharing
  - Collection limitation
  - Use limitation
  - Security and accountability



# OECD Fair Information Principles

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability
- <http://www.privacyrights.org/ar/fairinfo.htm>

# US FTC's Fair Information Practice Principles (FIPPs)

- Notice / Awareness
- Choice / Consent
- Access / Participation
- Integrity / Security
- Enforcement / Redress
- [https://en.wikipedia.org/wiki/FTC\\_Fair\\_Information\\_Practice](https://en.wikipedia.org/wiki/FTC_Fair_Information_Practice)



# Privacy on the Books / on the Ground

- Data Protection Directive (1995, since superseded by GDPR) - EU countries must adopt similar comprehensive laws, recognize privacy as fundamental human right
  - Privacy commissions in each country
- US has sector-specific laws, minimal protections, “patchwork quilt”
  - No explicit constitutional right to privacy or general privacy law
  - Some privacy rights inferred from constitution
  - Narrow regulations for health (HIPAA 1996), credit (FCRA 1970), education (FERPA 1974), video rental records (VPPA 1998), children (COPPA 1998)
  - FTC investigates **unfair & deceptive** practices
  - FCC regulates telecommunications
  - Some state and local laws
- See Bamberger and Mulligan, “Privacy on the Books and on the Ground,” <https://www.jstor.org/stable/41105400>

# General Data Protection Regulation (2016)

- **GDPR** came into effect May 25, 2018 and applies to the EU
- Distinguishes between data subjects, controllers (people who direct analysis), and processors (those who do the analysis)
- Data controller informs the 'data subject in a concise, **transparent**, intelligible and easily accessible form, using **clear and plain language**'
- **Right of access** for data subjects
- **Right of erasure** (with some exceptions)
- **Right to object** to processing for some purposes
- **Privacy by design** (Article 25)

# General Data Protection Regulation (2016)

- Pseudonymization required for stored personal data
- Data breach notification to authorities within 72 hours
- Possible fines of up to 4% of worldwide turnover
- Can only process data based on six lawful bases:
  - Consent
  - Contract
  - Public task
  - Vital interest
  - Legitimate interest
  - Legal requirement

# California Consumer Privacy Act (2018)

- **CCPA** went into effect January 1, 2020
- Residents of California have rights to:
  - Know what personal data is collected
  - Know whether that data is sold
  - Refuse the sale of personal data
  - Access their data
  - Request erasure of their personal data
  - Not be discriminated against for exercising these privacy rights
- Fine of \$7,500 for intentional and \$2,500 for unintentional violations

# Virginia Consumer Data Protection Act (2021)



The image is a screenshot of a news article from iapp. The article title is "Virginia passes the Consumer Data Protection Act". The date is "Mar 2, 2021" and there is a "Save This" button. The author is Sarah Rippy, an IAPP Staff Contributor. The article text discusses the signing of the Virginia Consumer Data Protection Act by Gov. Ralph Northam on March 2, 2021, and compares its substance to other privacy laws like the Washington Privacy Act and the California Consumer Privacy Act.

**iapp**

## Virginia passes the Consumer Data Protection Act

🕒 Mar 2, 2021 [Save This](#)

 Sarah Rippy  
IAPP Staff Contributor

After an extension into the 2021 special session, Gov. Ralph Northam, D-Va., signed the [Virginia Consumer Data Protection Act](#) into law March 2, 2021. In doing so, Virginia became the second state to enact comprehensive privacy legislation and the first to do so on its own initiative (California led the way in 2018. but the Legislature moved forward with the bill because they were facing a ballot initiative if they failed to do so).

The CDPA's substance is not particularly new compared to recent privacy laws. It draws heavily from the proposed Washington Privacy Act and includes components similar to the [California Consumer Privacy Act](#).

# Virginia Consumer Data Protection Act (2021)

- Slated to go into effect January 1, 2023
- “The bill applies to all persons that conduct business in the Commonwealth and either (i) control or process personal data of at least 100,000 consumers or (ii) derive over 50 percent of gross revenue from the sale of personal data and control or process personal data of at least 25,000 consumers.”
- “The bill grants **consumer rights to access, correct, delete, and obtain a copy of personal data and to opt out of the processing of personal data** for purposes of targeted advertising, the sale of personal data, or profiling of the consumer.”



# Tools of the FTC in the US

- Unfair practices
  - Injure consumer
  - Violate established policy
  - Unethical
- Deceptive practices
  - Mislead consumer
  - Differ from reasonable consumer expectations





The image is a screenshot of a web browser displaying the Federal Trade Commission's website. The browser's address bar shows "ftc.gov". The page features the FTC logo on the left, which includes a shield with scales of justice and the text "FEDERAL TRADE COMMISSION • UNITED STATES OF AMERICA". To the right of the logo, the text "FEDERAL TRADE COMMISSION" is written in large white letters, and "PROTECTING AMERICA'S CONSUMERS" is written in smaller light blue letters below it. A navigation bar at the bottom of the header contains a "MAIN MENU" link with a hamburger icon and a "SEARCH" link with a magnifying glass icon. The main content area has a white background and features a news article headline: "Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices". Below the headline is a sub-headline: "Settlement ensures consumers can control targeted ads". A blue box with the text "FOR RELEASE" is positioned below the sub-headline, followed by the date "December 20, 2016".

ftc.gov



**FEDERAL TRADE COMMISSION**  
PROTECTING AMERICA'S CONSUMERS

☰ MAIN MENU

🔍 SEARCH

## Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices

**Settlement ensures consumers can control targeted ads**

FOR RELEASE

December 20, 2016

# Privacy Issues

# Privacy Issues

- Can conflict with free speech / security
- A lack of privacy can cause chilling effects (discouragement of exercising a legitimate right)
- How do we provide transparency?
- Distortion: false or misleading information
- Value of data mining → future activities?
  - Limiting data collection can limit future the data's future value
- Oversight and accountability

# Measuring Privacy

- Why is privacy hard to measure?
- Why are attitudes about privacy hard to measure?
- Why is the cost of privacy invasion hard to measure?
- How do we quantify privacy harms?

# The Privacy Paradox

- When asked, we say we want privacy
- However, our behaviors make it seem like we don't care about privacy

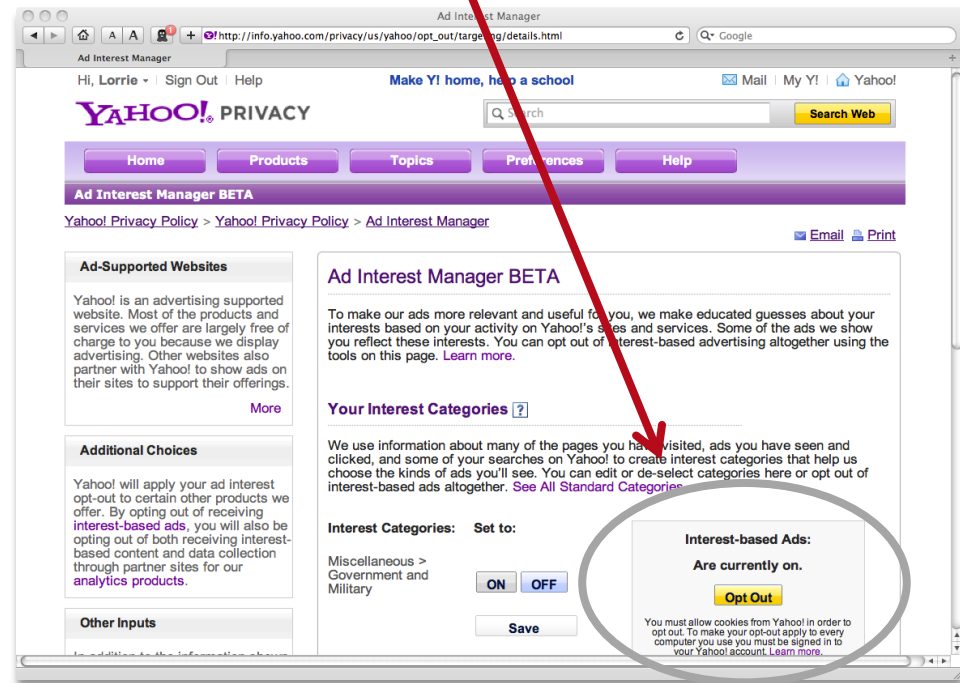
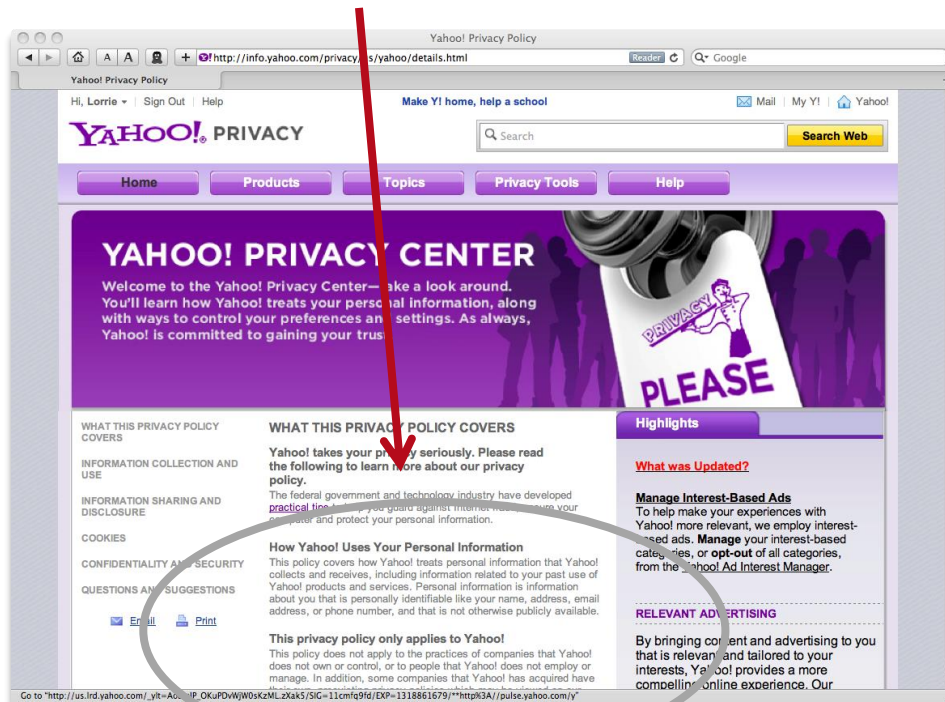
# **Communicating About Privacy**

# Notice and Choice

Protect privacy by giving people control over their information

**Notice** about data collection and use

**Choices** about allowing their data to be collected and used in that way





# Privacy Policies

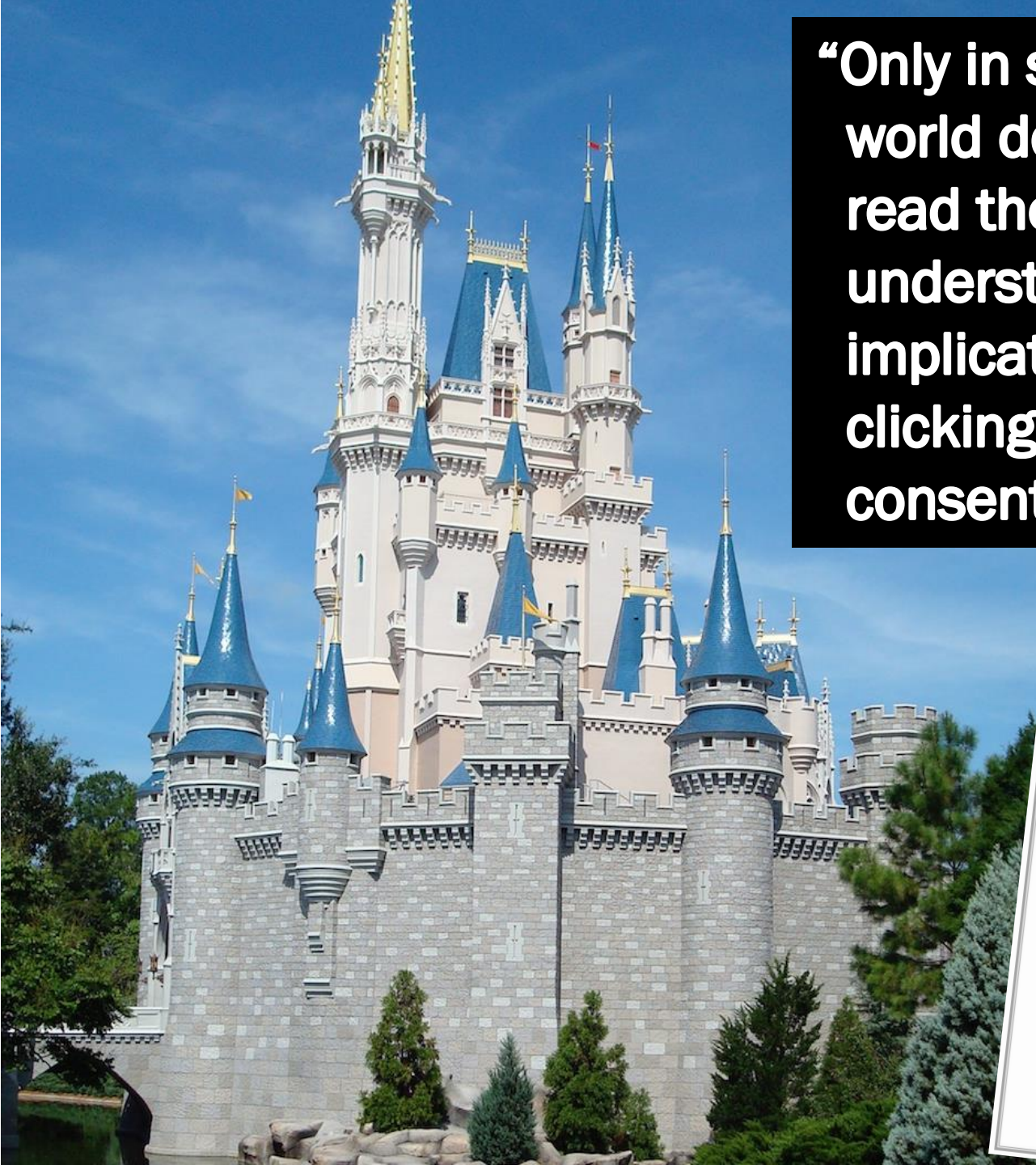
“the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand”

- *Protecting Consumer Privacy in an Era of Rapid Change*. Preliminary FTC Staff Report. December 2010.





**“Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent”**



**REPORT TO THE PRESIDENT  
BIG DATA AND PRIVACY:  
A TECHNOLOGICAL  
PERSPECTIVE**

Executive Office of the President  
President's Council of Advisors on  
Science and Technology

May 2014



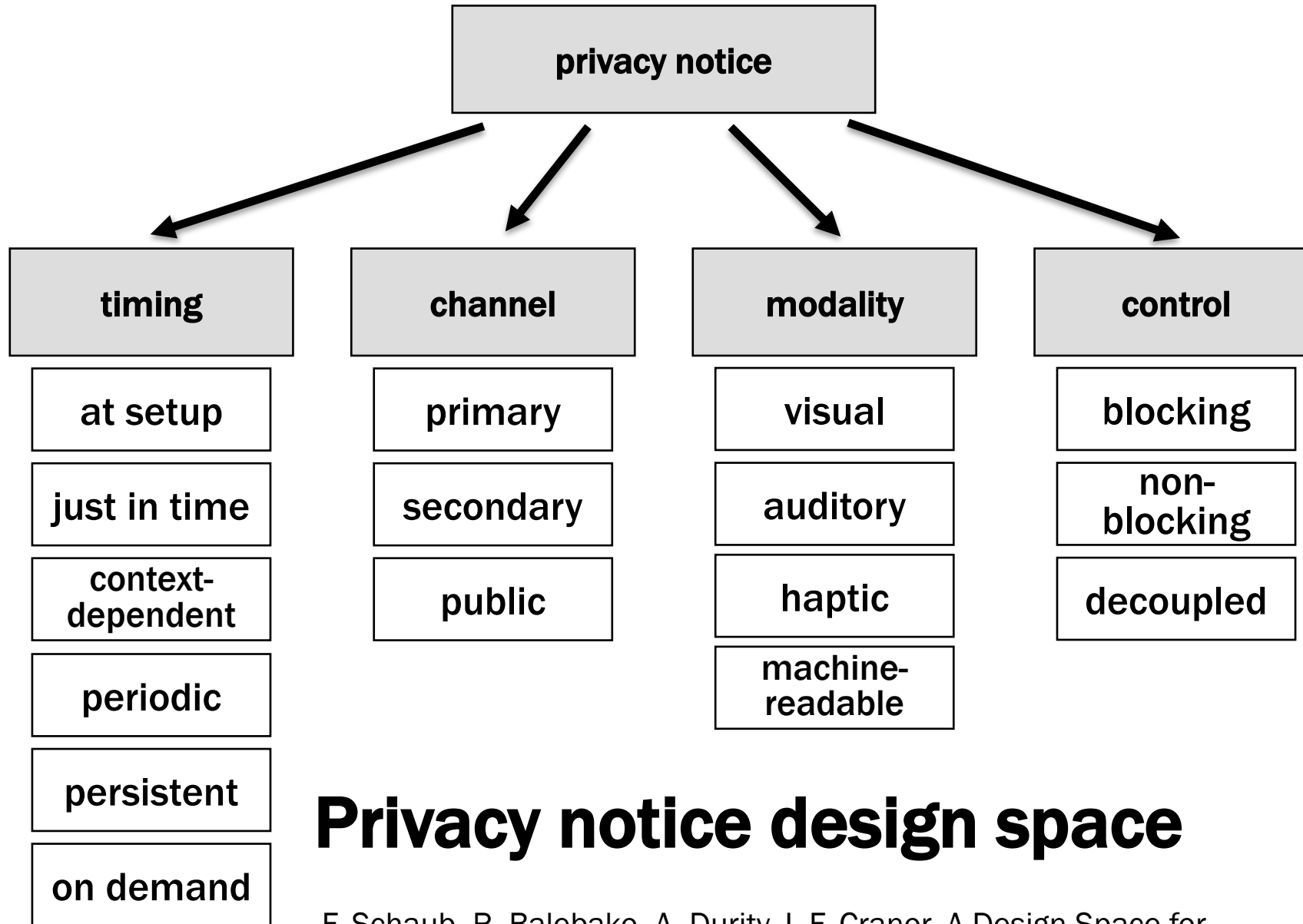
# Cost of Reading Privacy Policies

- What would happen if everyone read the privacy policy for each site they visited once per year?
- Time = 244/hours year
- Cost = \$3,534/year
- National opportunity cost for time to read policies: \$781 billion



Aleecia McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S:  
A Journal of Law and Policy for the Information Society. 2008 Privacy Year in Review Issue.

# **Privacy Notice Design Space**



## Privacy notice design space

F. Schaub, R. Balebako, A. Durity, L.F. Cranor, A Design Space for Effective Privacy Notices, SOUPS'15

# privacy notice

timing

channel

modality

control

at setup

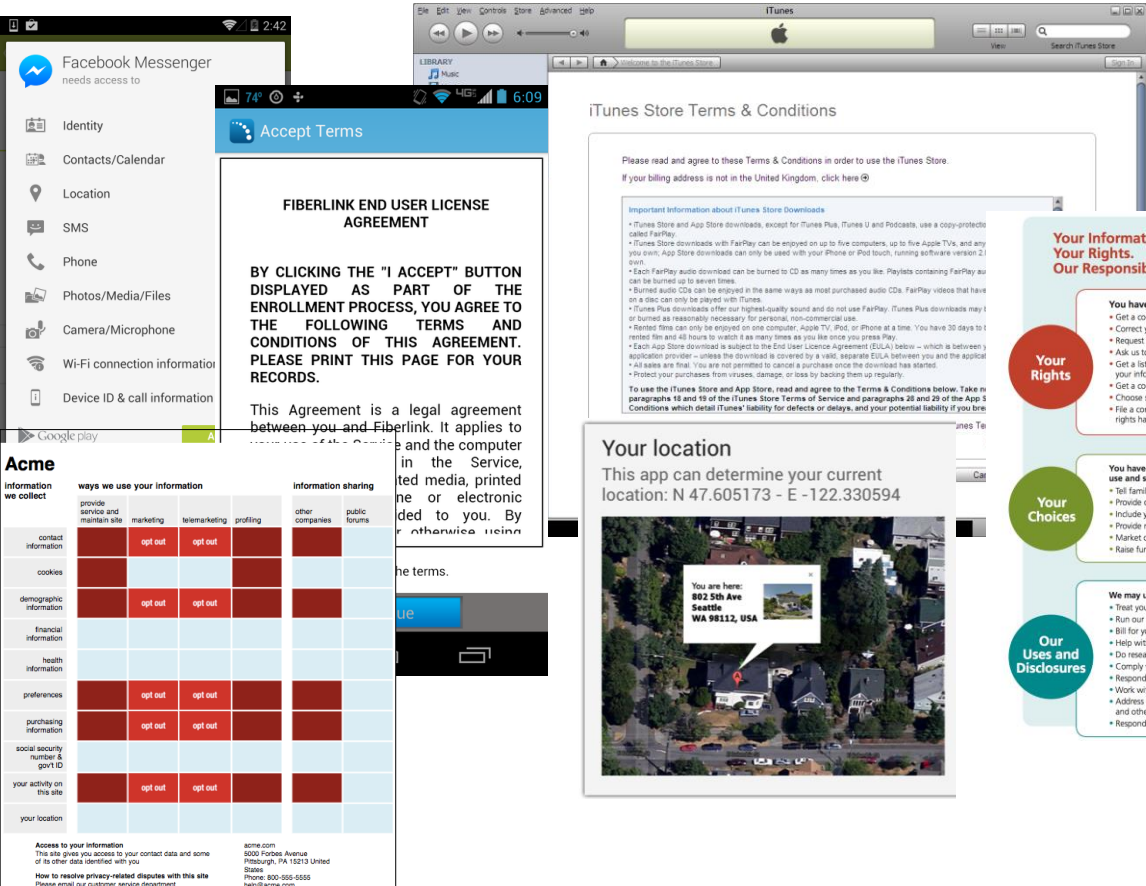
just in time

context-dependent

periodic

persistent

on demand



**Acme**  
Information we collect

ways we use your information	information sharing					
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

Access to your information  
This site gives you access to your contact data and some of other data identified with you.  
How to receive privacy-related notices with this site  
Please email our customer service department.

acme.com  
5000 Forbes Avenue  
Pittsburgh, PA 15213 United States  
Phone: 412-555-5555  
help@acme.com

**Your Information. Your Rights. Our Responsibilities.**

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. **Please review it carefully.**

**You have the right to:**

- Get a copy of your paper or electronic medical record
- Correct your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a list of those with whom we've shared your information
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

➤ See page 2 for more information on these rights and how to exercise them

**You have some choices in the way that we use and share information as we:**

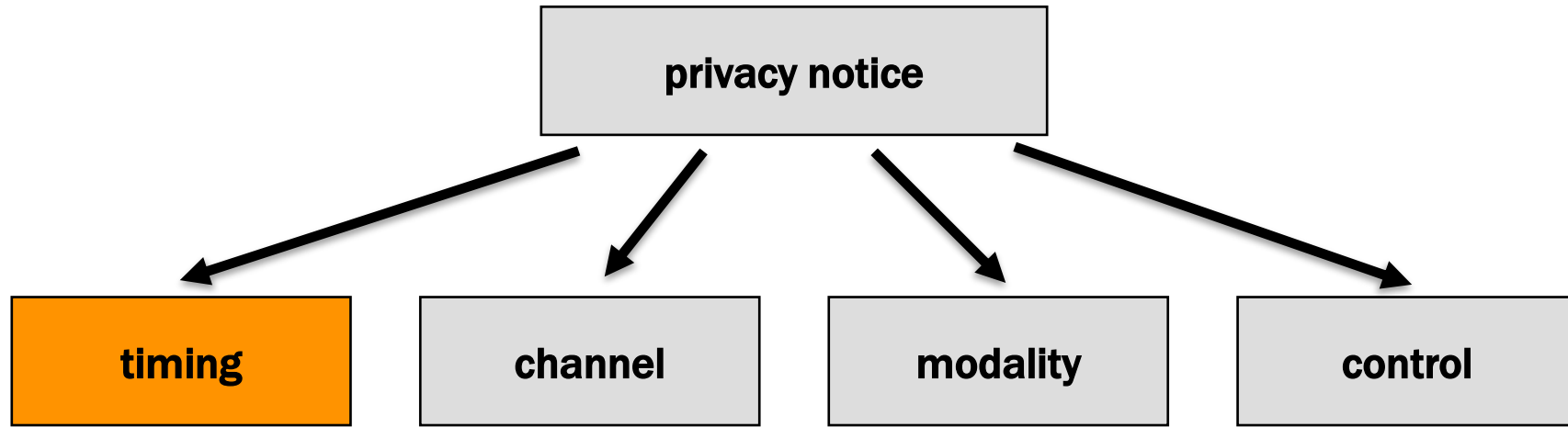
- Tell family and friends about your condition
- Provide disaster relief
- Include you in a hospital directory
- Provide mental health care
- Market our services and sell your information
- Raise funds

➤ See page 3 for more information on these choices and how to exercise them

**We may use and share your information as we:**

- Treat you
- Run our organization
- Bill for your services
- Help with public health and safety issues
- Do research
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner or funeral director
- Address workers' compensation, law enforcement, and other government requests
- Respond to lawsuits and legal actions

➤ See pages 3 and 4 for more information on these uses and disclosures



at setup

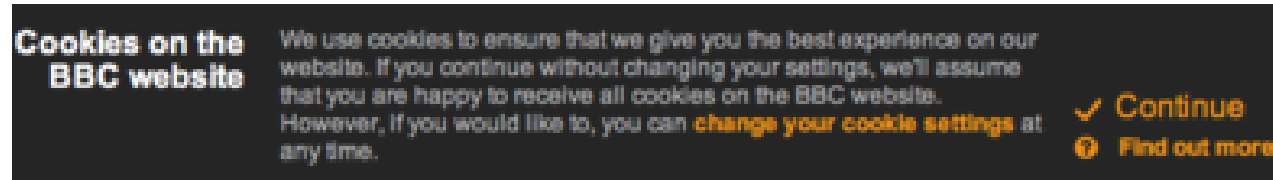
just in time

context-dependent

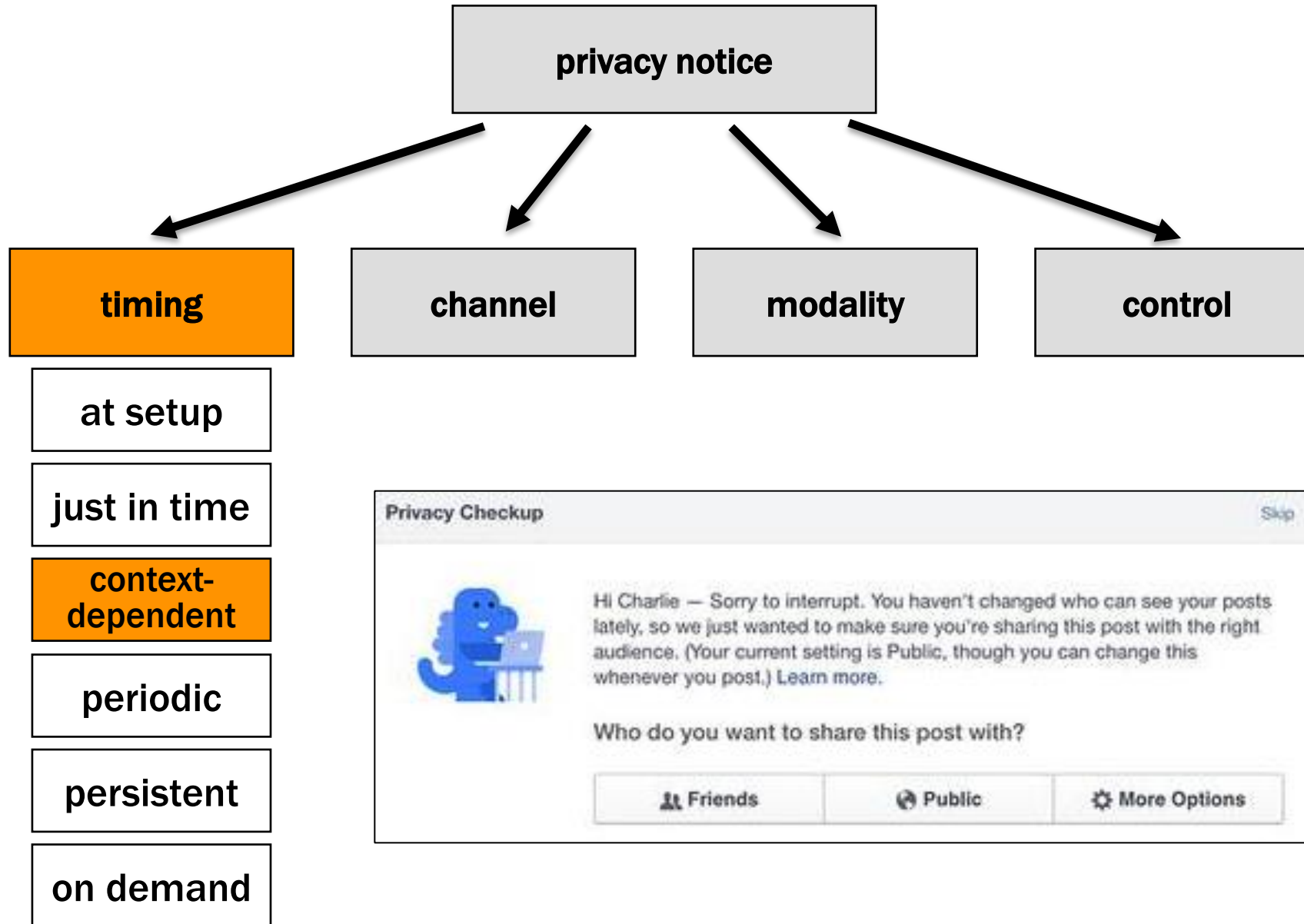
periodic

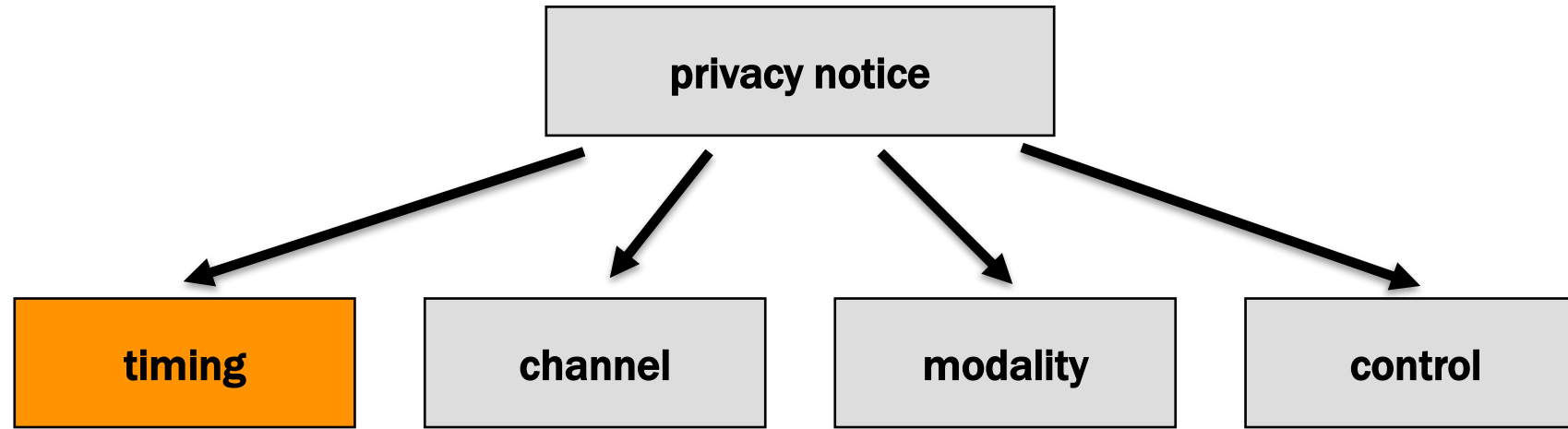
persistent

on demand

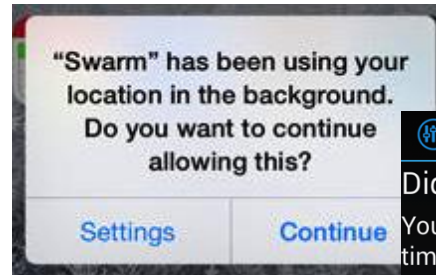








- at setup
- just in time
- context-dependent
- periodic**
- persistent
- on demand



Your location shared with 10 apps

Did you know?  
Your **location** has been shared **5398** times with Facebook, Groupon, GO Launcher EX, and 7 other apps for the past **14** days.

Let me change my settings

Show me more before I make changes

Keep sharing my location

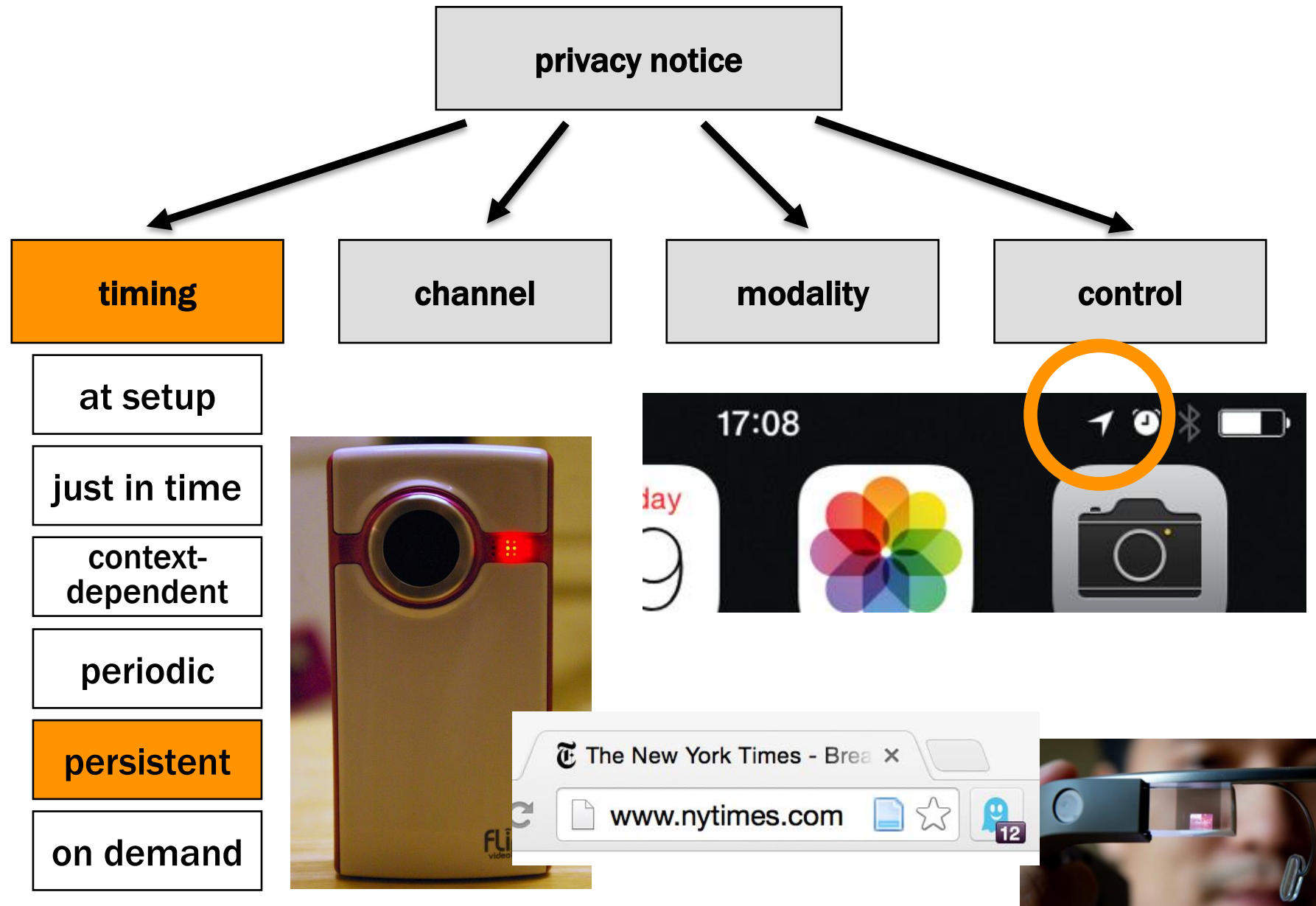
Notification provided by AppOps.

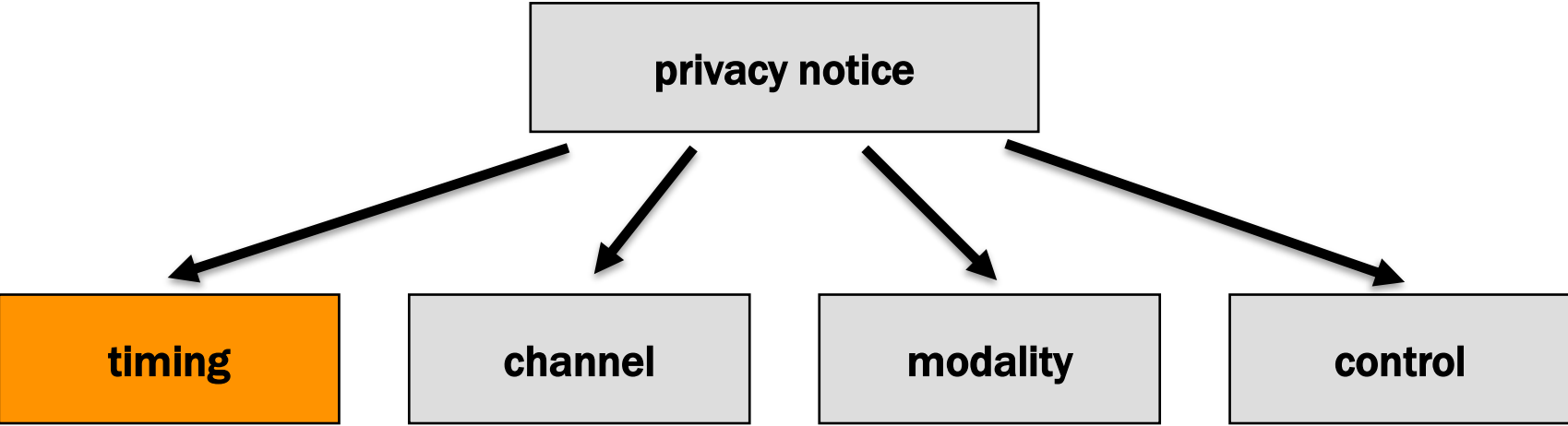
Rev. April 2015

FACTS	WHAT DOES PNC DO WITH YOUR PERSONAL INFORMATION?
<b>Why?</b>	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
<b>What?</b>	The types of personal information we collect and share depend on the product or service you have with us. This information can include: <ul style="list-style-type: none"> <li>• Social Security number and income</li> <li>• Account balances and account transactions</li> <li>• Credit scores and payment history</li> </ul>
<b>How?</b>	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information, the reasons PNC chooses to share, and whether you can limit this sharing.

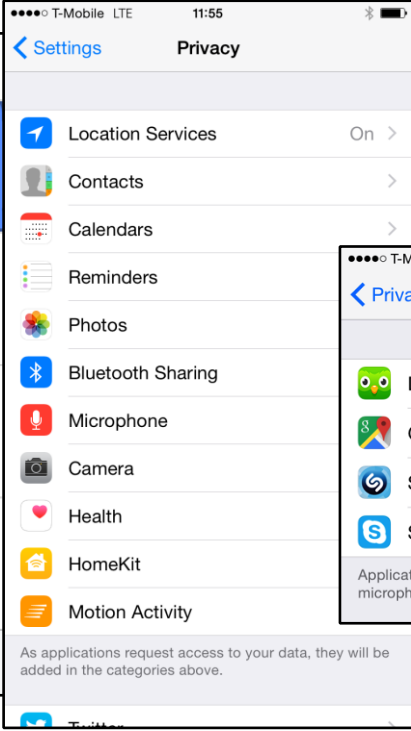
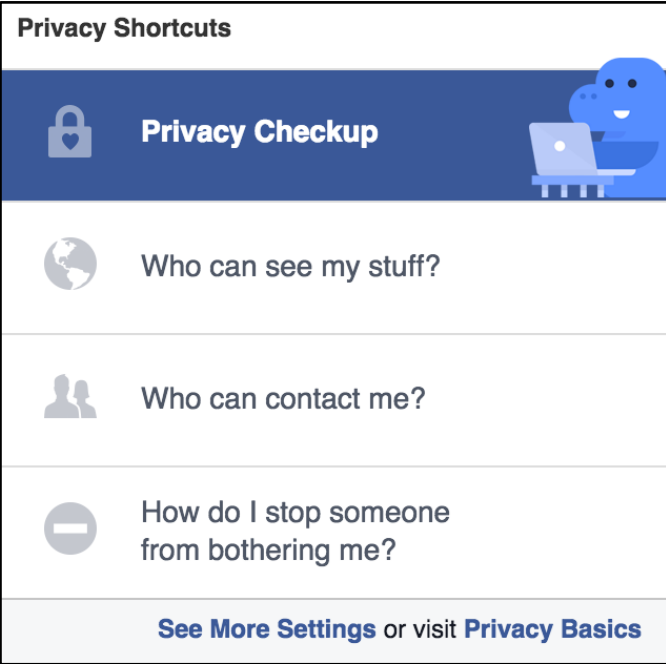
Reasons we can share your personal information	Does PNC share?	Can you limit this sharing?
<b>For our everyday business purposes</b> — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
<b>For our marketing purposes</b> — to offer our products and services to you	Yes	No
<b>For joint marketing with other financial companies</b>	Yes	Yes
<b>For our affiliates' everyday business purposes</b> — information about your transactions and experiences	Yes	No
<b>For our affiliates' everyday business purposes</b> — information about your creditworthiness	Yes	Yes
<b>For our affiliates to market to you</b>	Yes	Yes
<b>For nonaffiliates to market to you</b>	No	We don't share

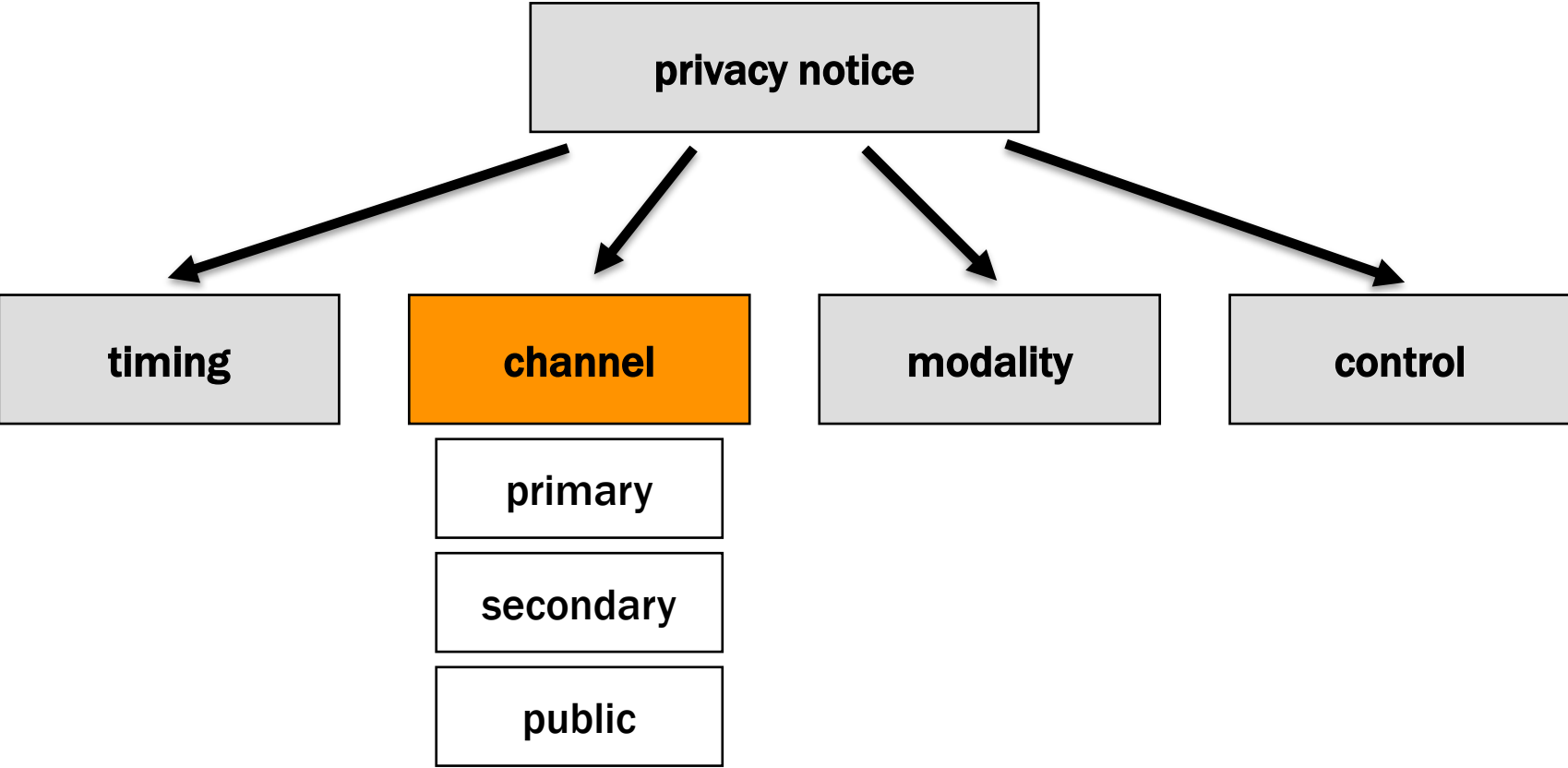
<b>To limit our sharing</b>	<ul style="list-style-type: none"> <li>• Call 1-800-762-2118 — our menu will prompt you through your choice(s)</li> <li>• Visit us online: <a href="http://www.PNC.com/privacy">www.PNC.com/privacy</a> (Online Banking customers only)</li> </ul> <p><b>Please note:</b> If you are a new customer, we can begin sharing your information 30 days from the date we sent this notice. When you are <i>no longer</i> our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.</p>
<b>Questions?</b>	Call 1-800-762-2118

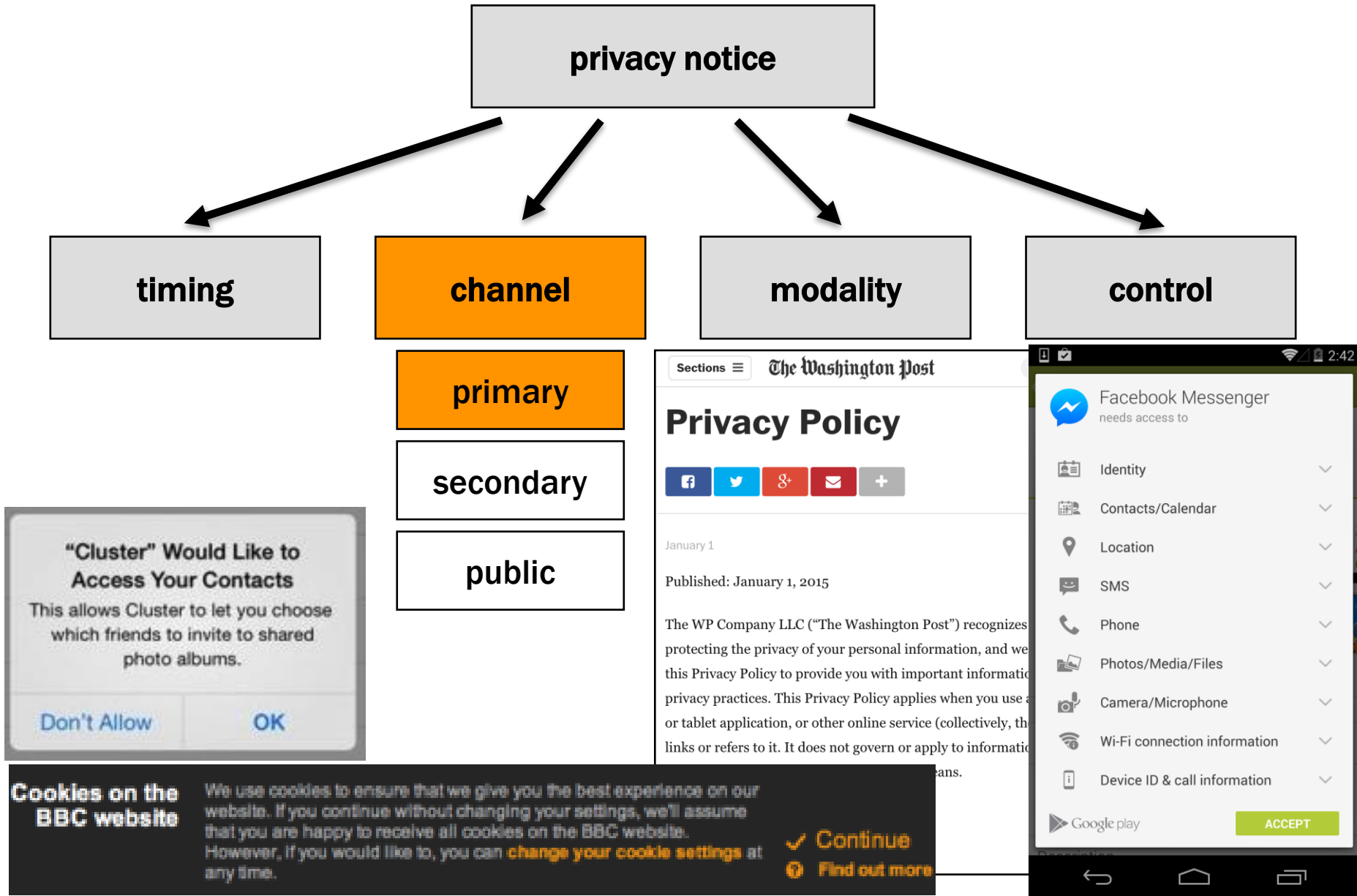




- at setup
- just in time
- context-dependent
- periodic
- persistent
- on demand







**"Cluster" Would Like to Access Your Contacts**  
This allows Cluster to let you choose which friends to invite to shared photo albums.

Don't Allow      OK

**Cookies on the BBC website** We use cookies to ensure that we give you the best experience on our website. If you continue without changing your settings, we'll assume that you are happy to receive all cookies on the BBC website. However, if you would like to, you can **change your cookie settings** at any time.

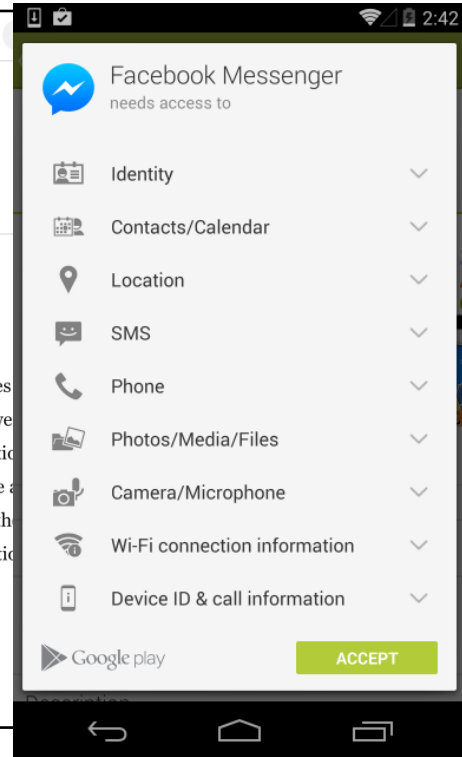
Continue      Find out more

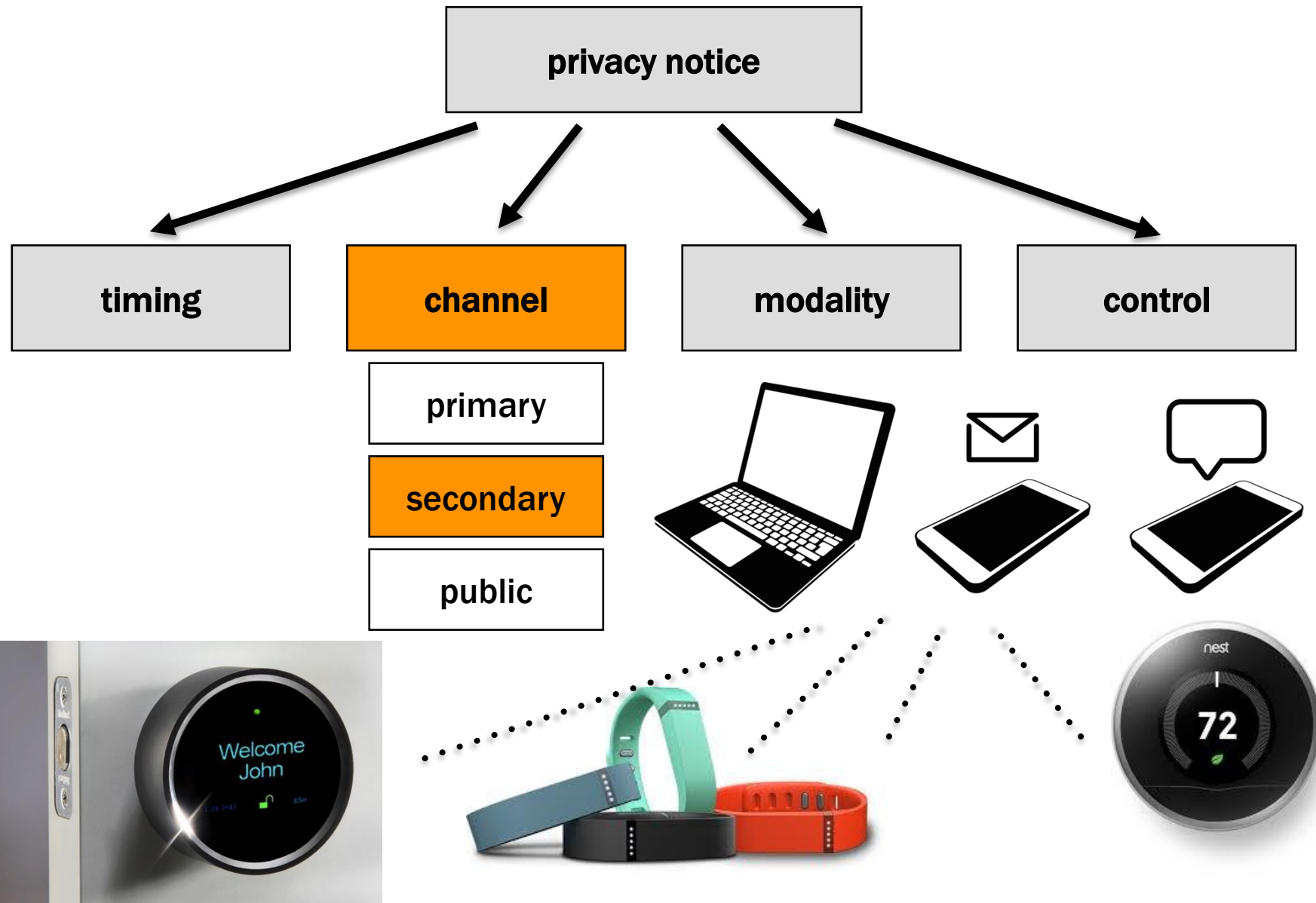
Sections    The Washington Post

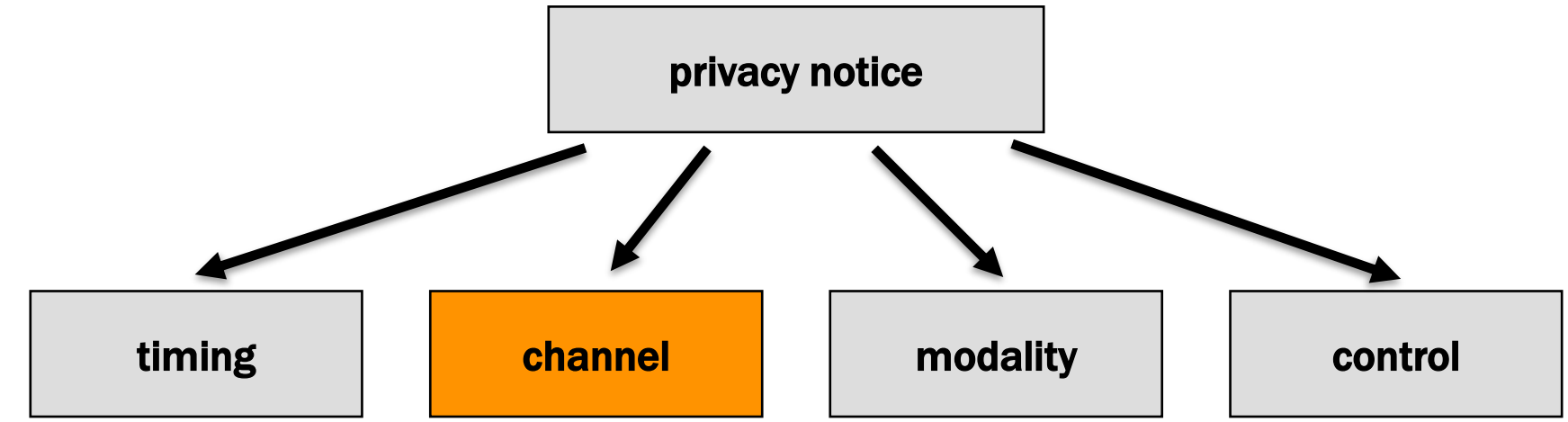
### Privacy Policy

January 1  
Published: January 1, 2015

The WP Company LLC ("The Washington Post") recognizes protecting the privacy of your personal information, and we this Privacy Policy to provide you with important information privacy practices. This Privacy Policy applies when you use or tablet application, or other online service (collectively, the links or refers to it. It does not govern or apply to information





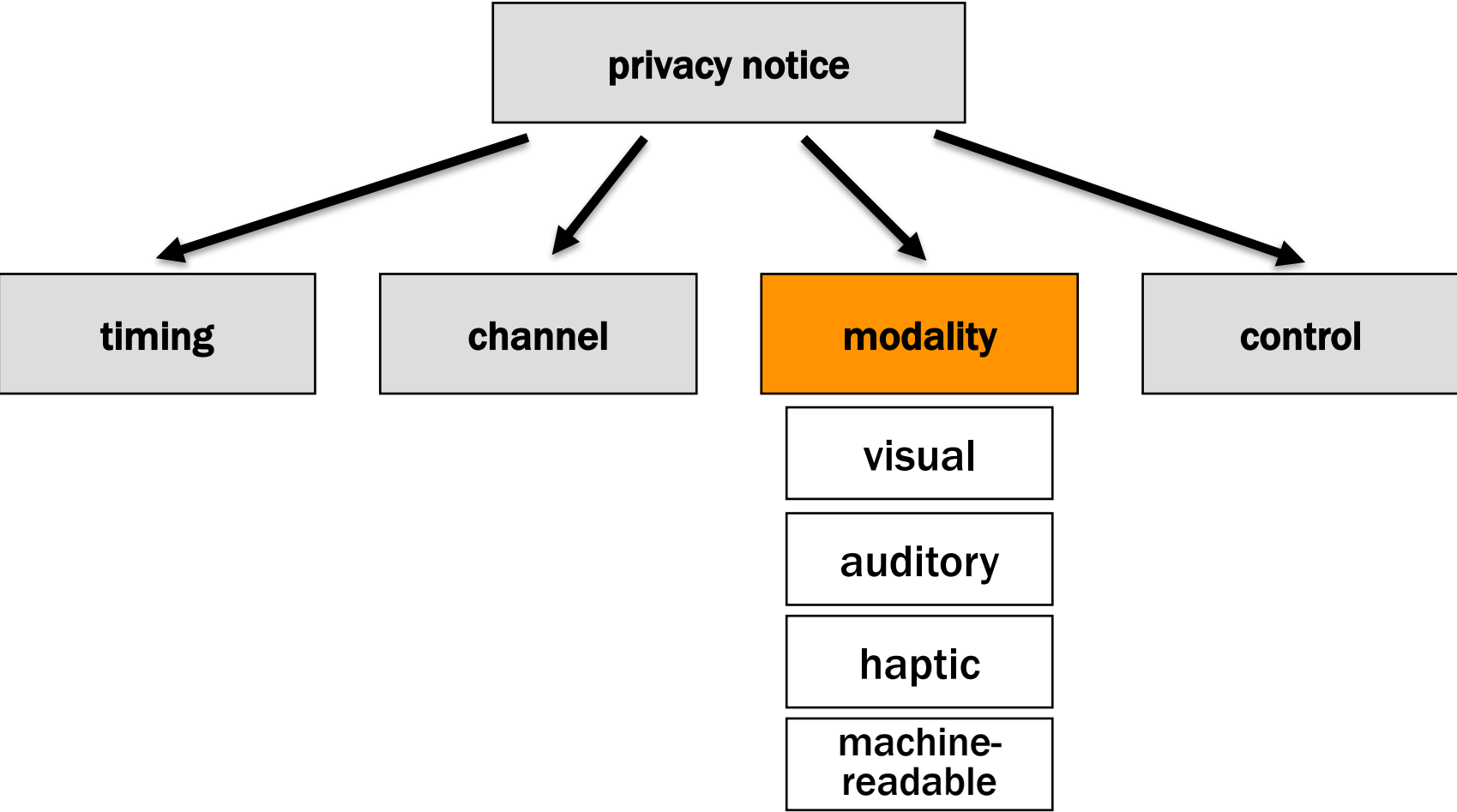


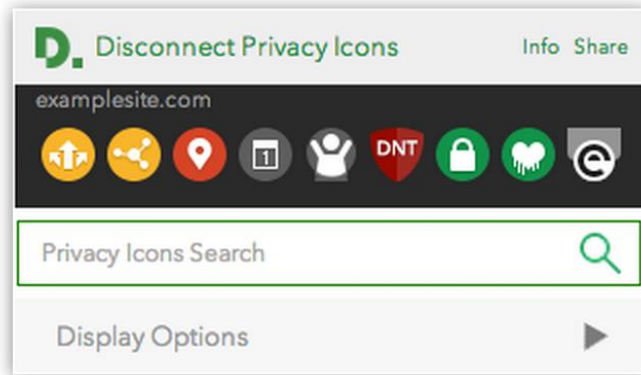
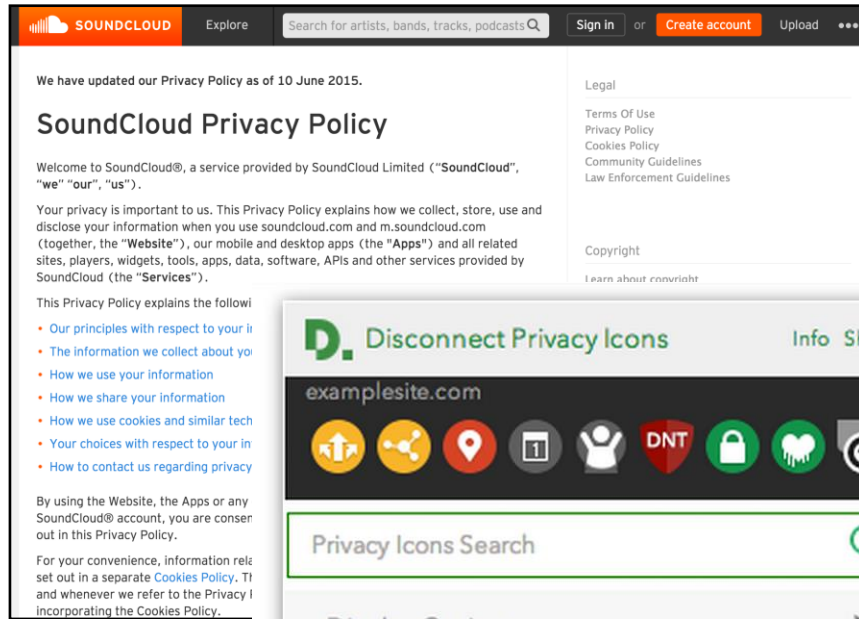
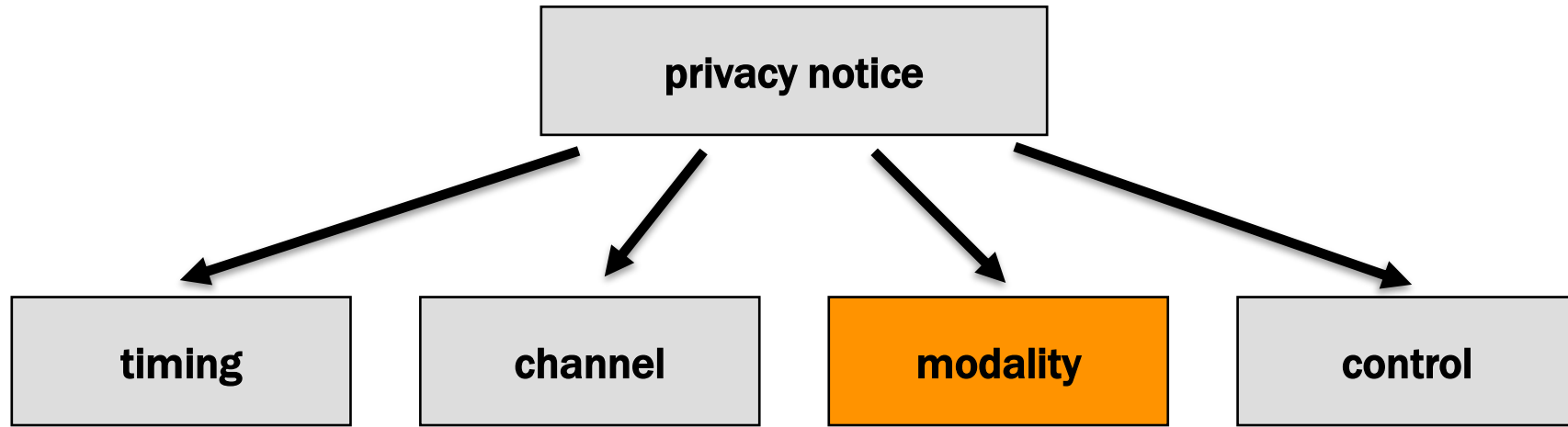
- primary
- secondary
- public**



<http://www.offlinetags.net/>

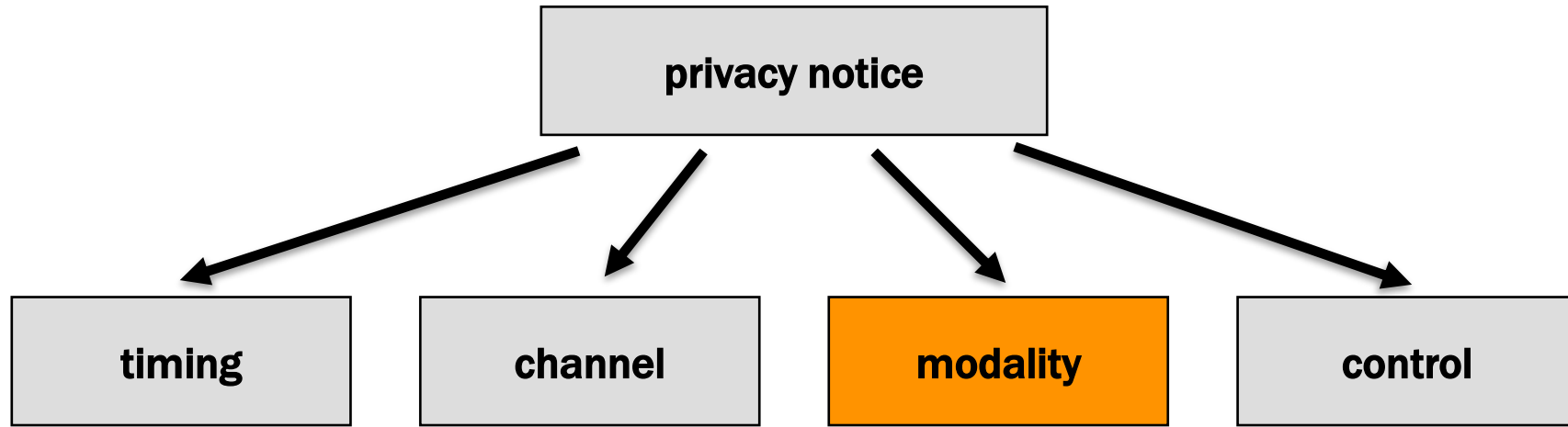






- visual
- auditory
- haptic
- machine-readable



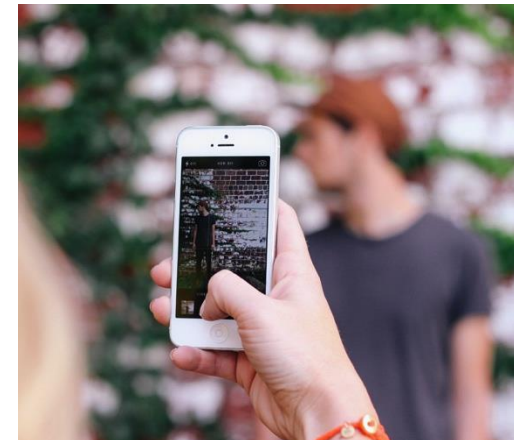


visual

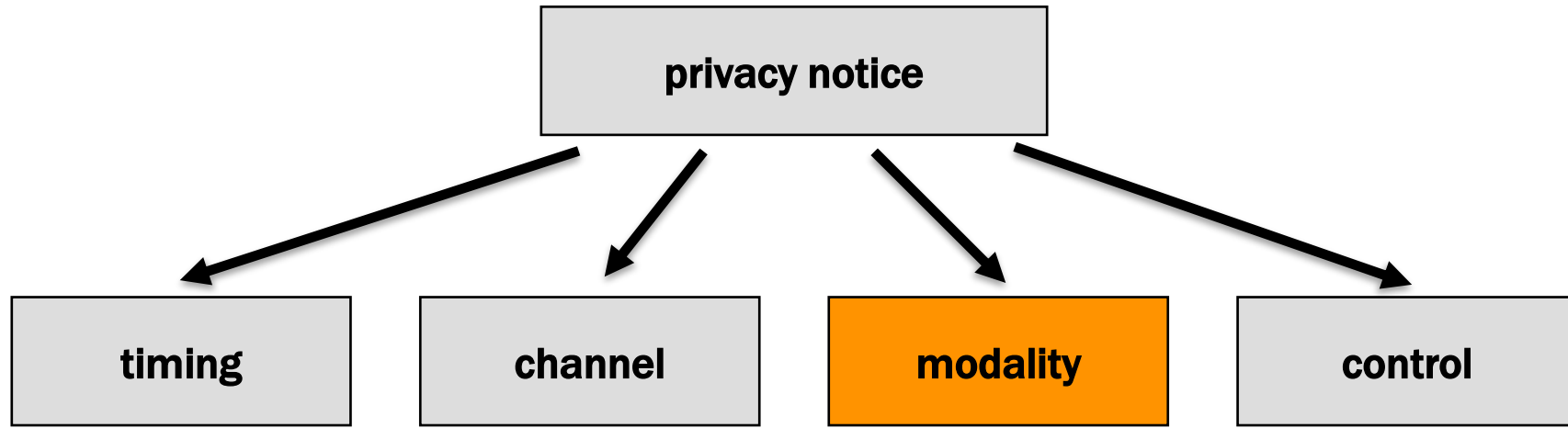
auditory

haptic

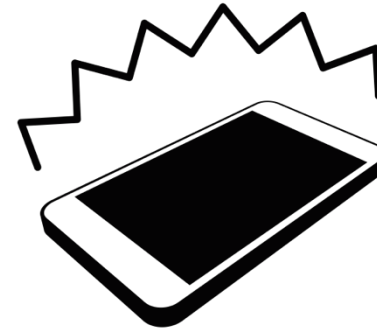
machine-readable

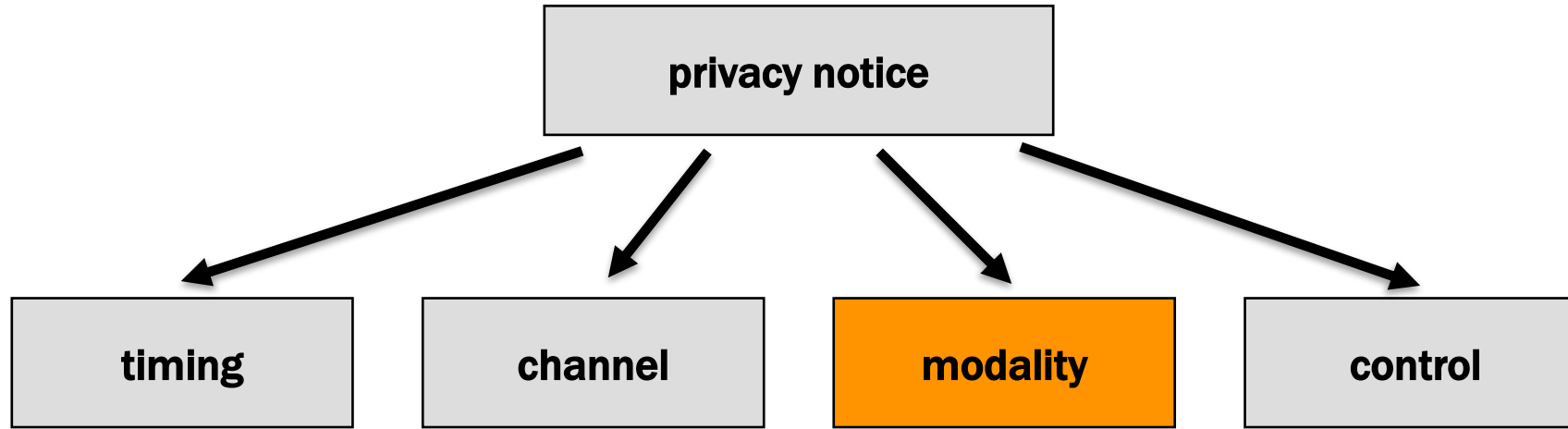


*“this call will be recorded for training purposes”*



- visual
- auditory
- haptic**
- machine-readable





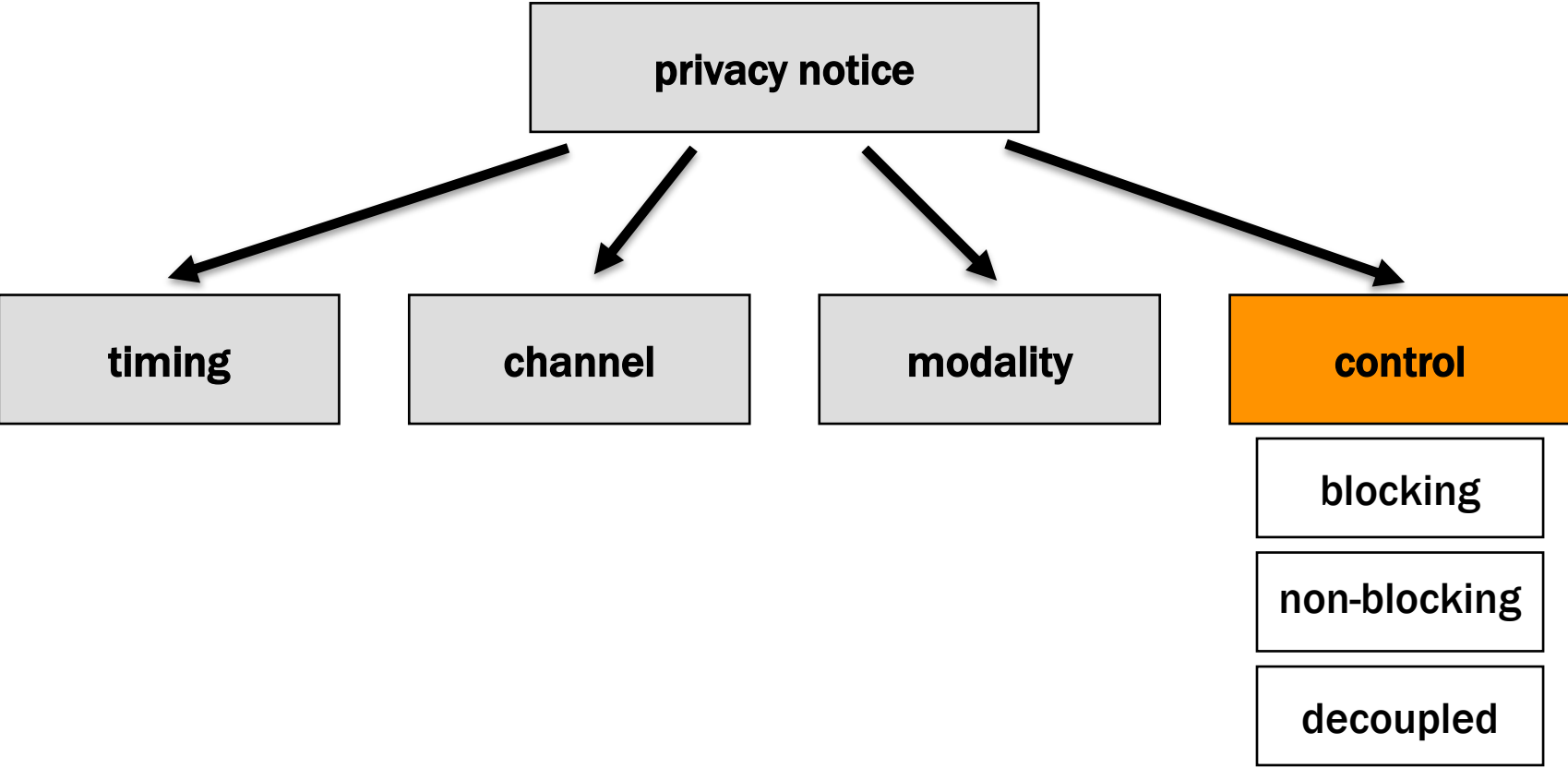
The Platform for Privacy Preferences 1.1 (P3P1.1) Specification  
 W3C Working Group Note 13 November 2006

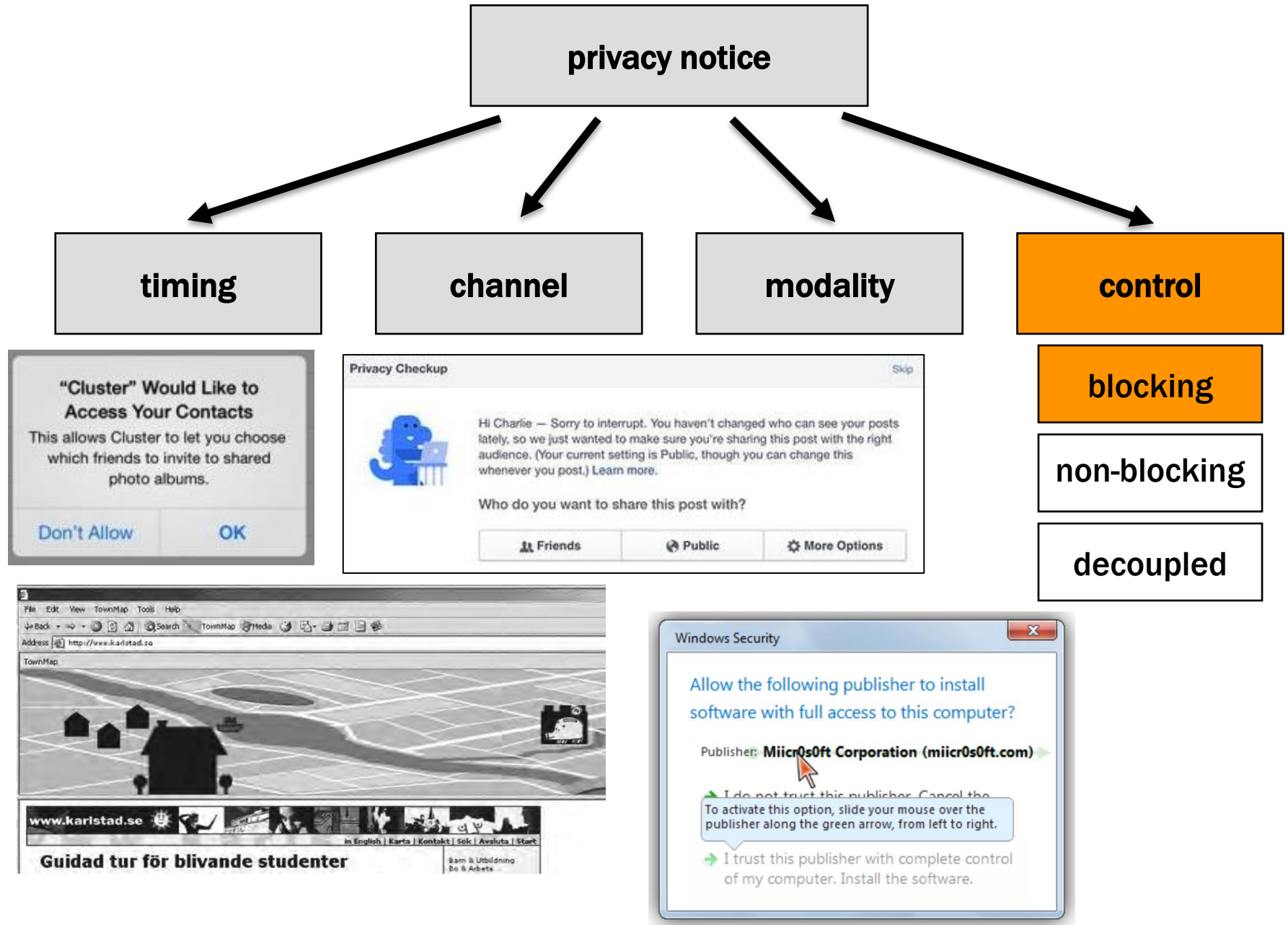


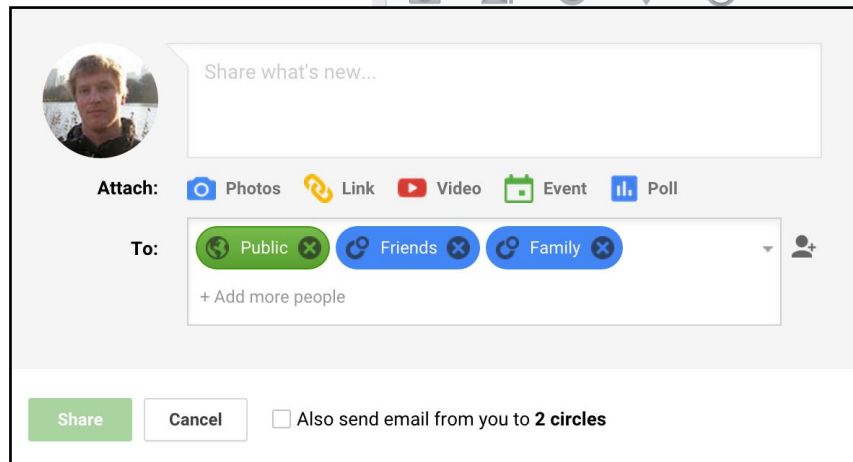
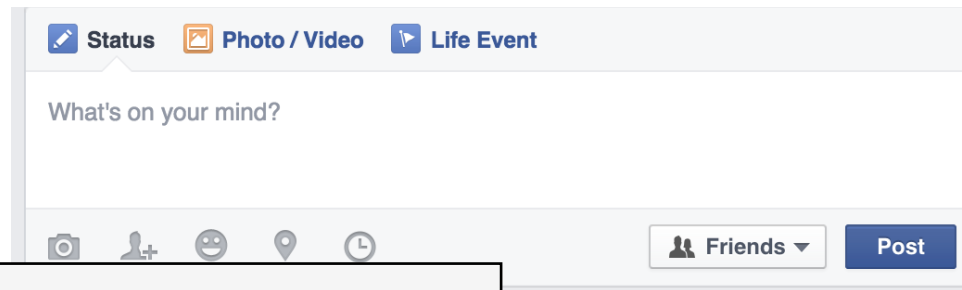
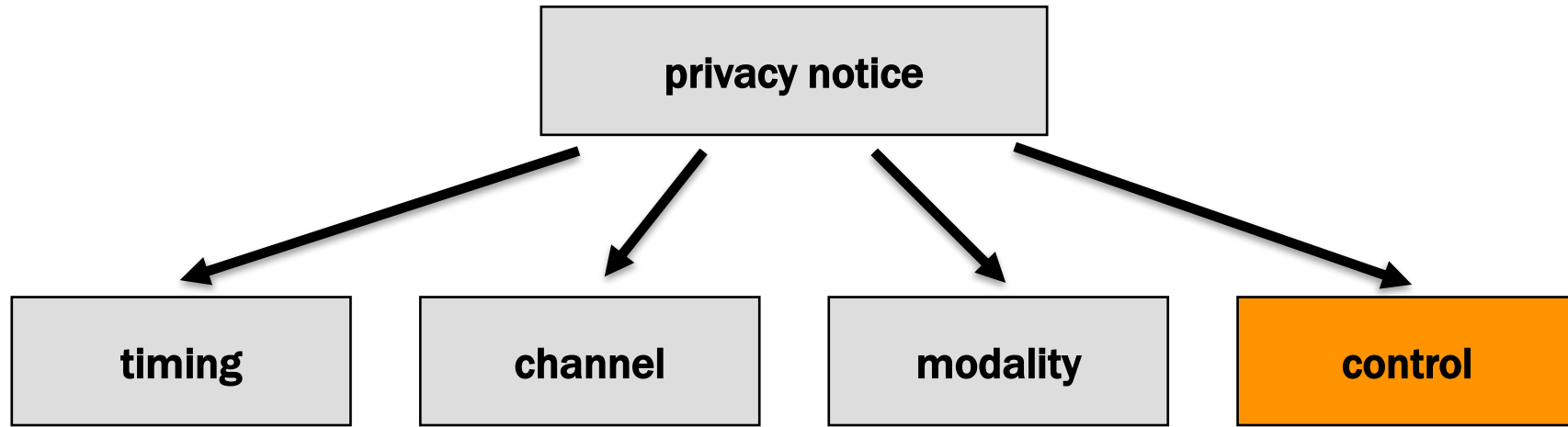
- visual
- auditory
- haptic
- machine-readable

```

<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
  entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
      description="PrivacySeal, a third-party seal provider"
      image="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
    <CONSEQUENCE-GROUP>
      <CONSEQUENCE>a site with clothes you would appreciate</CONSEQUENCE>
    </CONSEQUENCE-GROUP>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <PURPOSE><custom/><develop/></PURPOSE>
    <DATA-GROUP>
      <DATA name="dynamic.cookies" category="state"/>
      <DATA name="dynamic.miscdata" category="preference"/>
      <DATA name="user.gender"/>
      <DATA name="user.home." optional="yes"/>
    </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/><develop/></PURPOSE>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="dynamic.clickstream.server"/>
      <DATA name="dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
  
```

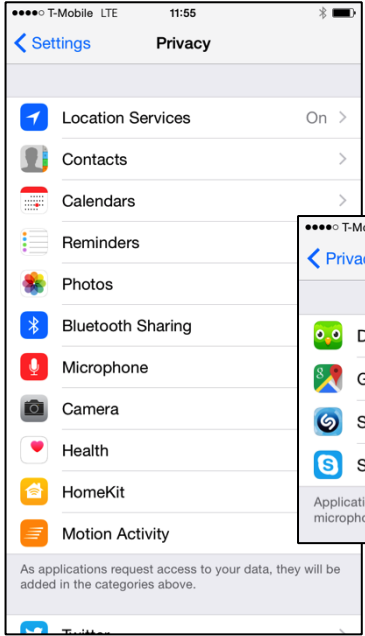
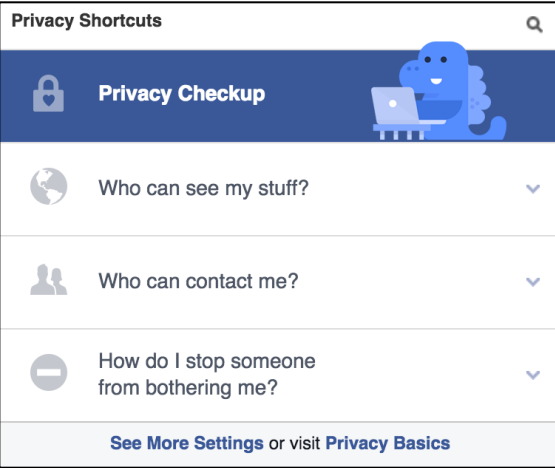
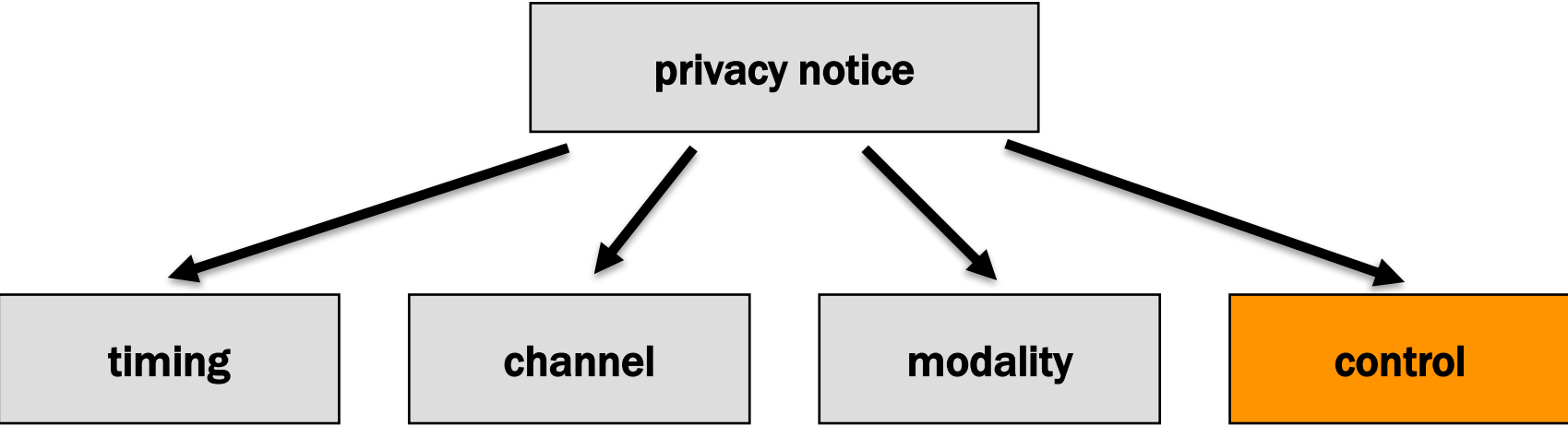






- blocking
- non-blocking
- decoupled





- blocking
- non-blocking
- decoupled

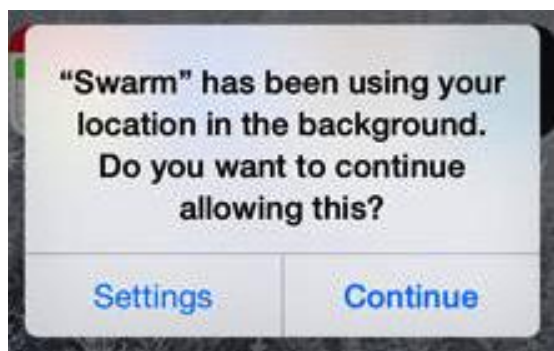
# Layered Examples (iOS)



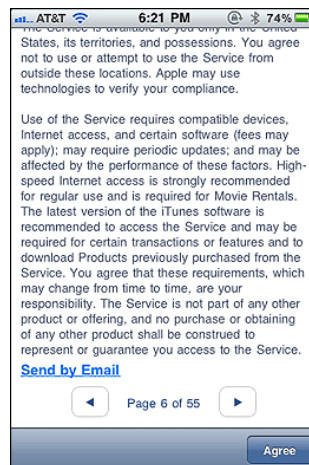
just-in-time, primary visual, blocking



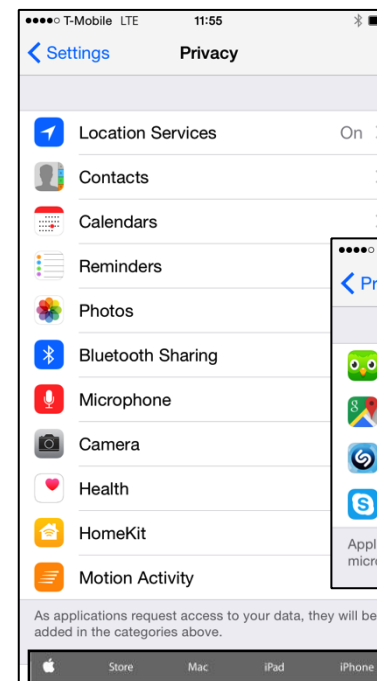
persistent, primary visual, non-blocking



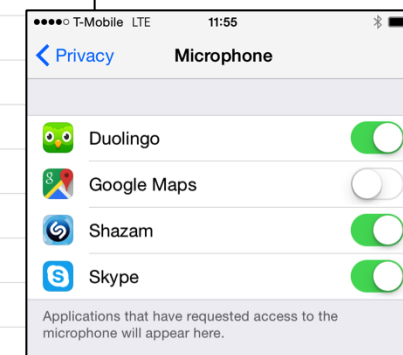
periodic, primary visual, blocking



at setup, primary visual, blocking



on demand, primary visual, decoupled

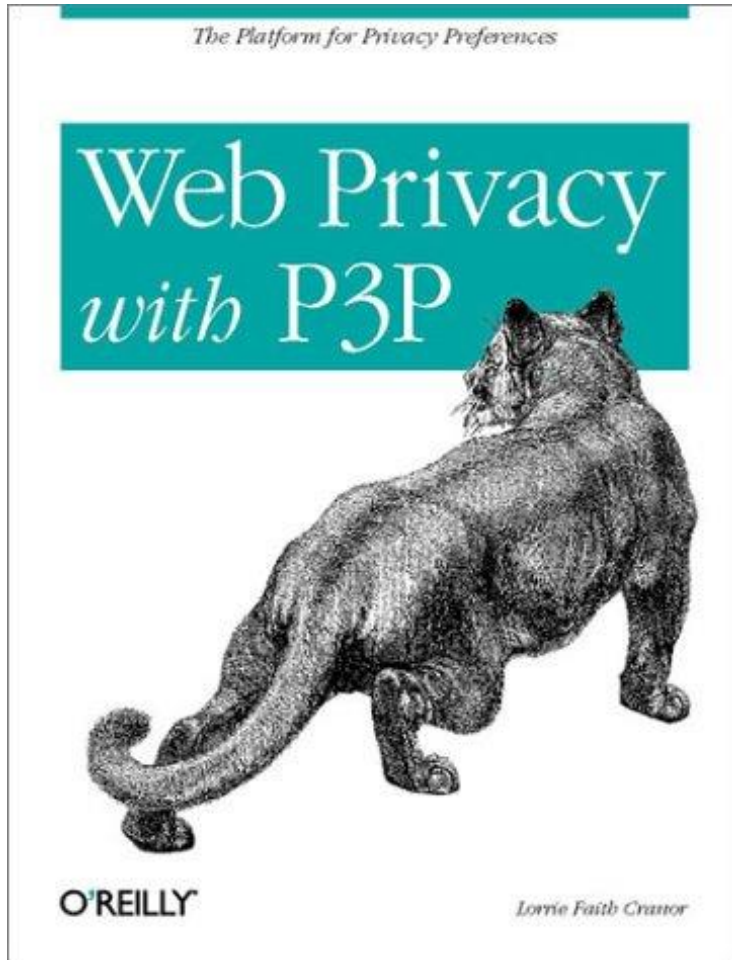


on demand, secondary visual, decoupled

# **Attempts at improving notice & choice**

# **Attempt: Machine-readable privacy policies**

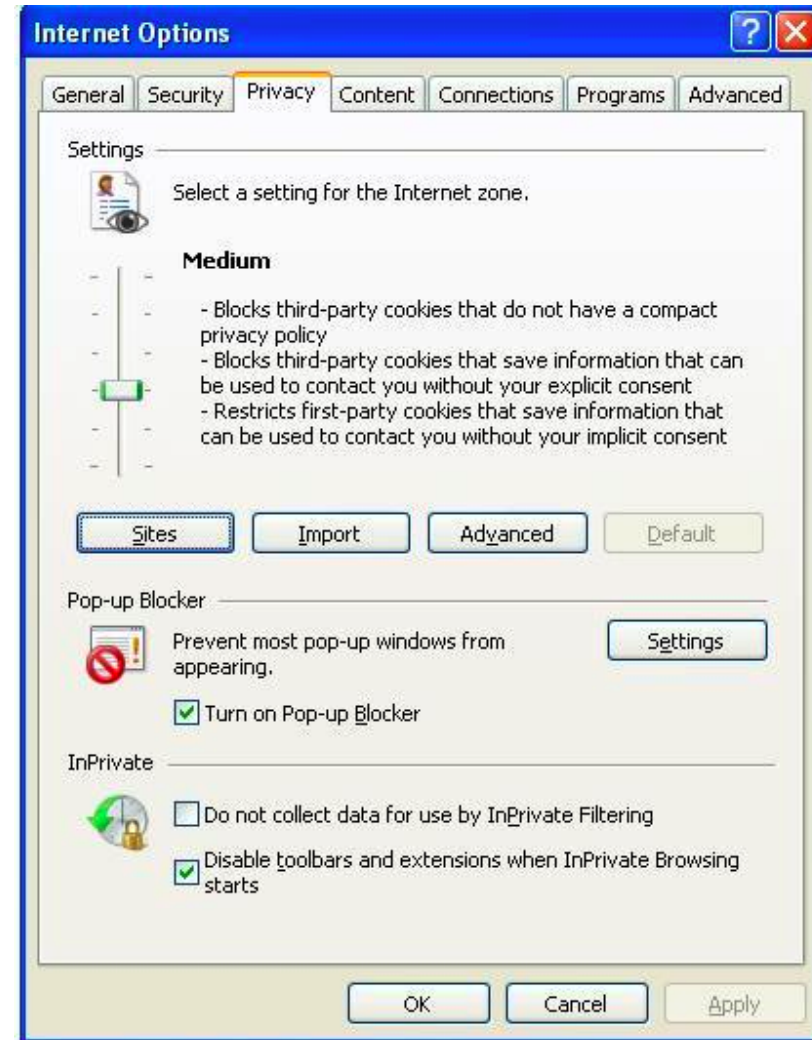
# Let your computer read for you



- Platform for Privacy Preferences (P3P)
- W3C specification for XML privacy policies
  - Proposed 1996
  - Adopted 2002
- Optional P3P compact policy HTTP headers to accompany cookies
- Lacks incentives for adoption

# P3P in Internet Explorer

- P3P implemented in IE 6, 7, 8, 9, 10 ...
- Default privacy setting
  - Rejects third-party cookies without a CP
  - Rejects unsatisfactory third-party cookies



**Attempt: Make your own  
machine-readable privacy  
policies**

# Use NLP to read policies






- Usableprivacy.org
- It's a hard problem
- Annotated corpus → machine learning



# **Attempt: Crowdsourcing**






# Terms of Service; Didn't Read

## SoundCloud Class B

-  You stay in control of your copyright
-  Collected personal data used for limited purposes
-  6 weeks to review changes
-  Indemnification from claims related to your content or your account
-  Personal information can be disclosed in case of business transfer or insolvency






 [More details](#)

## GitHub Class B

-  You don't grant any copyright license to github
-  Changes can happen any time, sometimes without notice
-  You shall defend and indemnify GitHub
-  Your personal information is used for limited purposes
-  Your account can be suspended and your data deleted any time for any reason






 [More details](#)

## Twitpic Class E

-  Twitpic takes credit for your content
-  Your content is for Twitpic and their partners
-  Reduction of legal period for cause of action
-  You indemnify Twitpic from any claim related to your content
-  Deleted images are not really deleted

 [More details](#)

## Delicious Class D

-  Very broad copyright license on your content, includes right for Delicious to distribute through any media
-  No Right to leave the service
-  Only for personal and non-commercial use
-  [bad] delicious new terms 5. third party services get access to personal information
-  Your personal information are an asset for business transfers

 [More details](#)

# **Attempt: Standardized notices**

**Privacy Facts**

[Redacted text block]

**Privacy Facts**

[Redacted text block]

**Privacy Facts**

[Redacted text block]

**Privacy Facts**

[Redacted text block]

# Privacy nutrition labels

- Series of studies
  - Focus groups
  - Lab studies
  - Online studies
- Metrics
  - Reading-comprehension (accuracy)
  - Time to find information
  - Ease of policy comparison
  - Subjective opinions, ease, fun, trust

P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder. A “Nutrition Label” for Privacy. SOUPS 2009.

P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CHI 2010.





**Acme**

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

**Access to your information**  
This site gives you access to your contact data and some of its other data identified with you

**How to resolve privacy-related disputes with this site**  
Please email our customer service department

acme.com  
5000 Forbes Avenue  
Pittsburgh, PA 15213 United States  
Phone: 800-555-5555  
help@acme.com

	we will collect and use your information in this way		we will not collect and use your information in this way
	by default, we will collect and use your information in this way unless you tell us not to by opting out		by default, we will not collect and use your information in this way unless you allow us to by opting in

# Standardized financial notices

- Gramm-Leach-Bliley Act mandated annual disclosures
- In 2009, regulators created a recommended form
  - High adoption because of safe harbor

# Standardized financial notices

Rev. [insert date]

## FACTS

WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?

### Why?

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

### What?

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and [income]
- [account balances] and [payment history]
- [credit history] and [credit scores]

When you are *no longer* our customer, we continue to share your information as described in this notice.

### How?

All financial companies need to share **customers'** personal information to run their everyday business. In the section below, we list the reasons financial companies can share their **customers'** personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

# Standardized financial notices

Reasons we can share your personal information	Does [name of financial institution] share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes – to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes – information about your transactions and experiences		
For our affiliates' everyday business purposes – information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		
<b>Questions?</b>	Call [phone number] or go to [website]	



# Standardized financial notices

Page 2	
Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of financial institution] protect my personal information?	<p>To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.</p> <p>[insert]</p>
How does [name of financial institution] collect my personal information?	<p>We collect your personal information, for example, when you</p> <ul style="list-style-type: none"><li>■ [open an account] or [deposit money]</li><li>■ [pay your bills] or [apply for a loan]</li><li>■ [use your credit or debit card]</li></ul> <p>[We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]</p>
Why can't I limit all sharing?	<p>Federal law gives you the right to limit only</p> <ul style="list-style-type: none"><li>■ sharing for affiliates' everyday business purposes—information about your creditworthiness</li><li>■ affiliates from using your information to market to you</li><li>■ sharing for nonaffiliates to market to you</li></ul> <p>State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]</p>

# Standardized financial notices

Definitions	
<b>Affiliates</b>	<p>Companies related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"><li>■ <i>[affiliate information]</i></li></ul>
<b>Nonaffiliates</b>	<p>Companies not related by common ownership or control. They can be financial and nonfinancial companies.</p> <ul style="list-style-type: none"><li>■ <i>[nonaffiliate information]</i></li></ul>
<b>Joint marketing</b>	<p>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.</p> <ul style="list-style-type: none"><li>■ <i>[joint marketing information]</i></li></ul>
Other important information	
<i>[insert other important information]</i>	

# Standardized financial notices

- Built a parser and built an online database
- Lets people compare practices
- <https://cups.cs.cmu.edu/bankprivacy>

**Attempt: Improve timing**

# Privacy label for Android

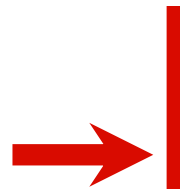
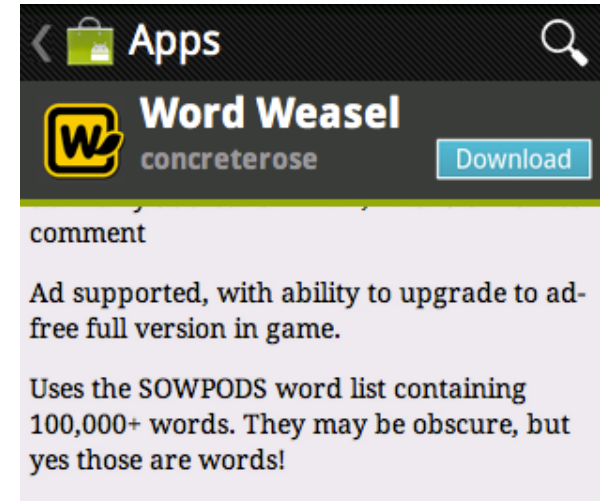


**Privacy score** ★★★★☆ 793  
10,000+ downloads  
1.9MB

## DESCRIPTION

Like word games? Like weasels? This is the game for you. Word Weasel is a fast word game where you find as many words as you can from 9 letters in 50 seconds. Compete with everyone else playing at the same time, a new game starts every minute!

"The most fun you can have on your own with 9 random letters. Brilliantly simple, devilishly addictive." --Kim, Android Market comment



## Privacy Facts

THIS APP COLLECTS YOUR

- Personal information
- Contacts
- Location
- Calendars
- Credit card / financial
- Diet / nutrition
- Health / medical
- Photos

THIS APP USES

- Advertising
- Analytics

## REVIEWS



# **Attempt: Personalized privacy assistants**

# Personal privacy assistants



**Attempt: Icons**





# **Attempt: Standardized disclosure icons**

AdChoices 



Pop in. Stand out.

Buy Now!

 **TARGET**  **P&G eStore**  
by eStore Retail Services  **amazon.com**

**AT&T.**  
The nation's  
**largest**  
**4G**  
**network.**



**LEARN MORE**

Rethink Possible® 

4G speeds not available everywhere.

It's 1702, a decade after  
*The Crucible's* infamous seductress  
danced with the devil in Salem.

MAY 4-26, 2013

*Abigail*  
1702

BY ROBERTO AGUIRRE-SACASA  
DIRECTED BY TRACY BRIGDEN

**CITY THEATRE**

**BUY TICKETS >**

**YAHOO!**  
--- ON THE ---  
**ROAD**

**Don't miss a beat**

Ad Feedback

AdChoices 