UMBC

Dr. Roberto Yus

https://robertoyus.com/

Data Privacy

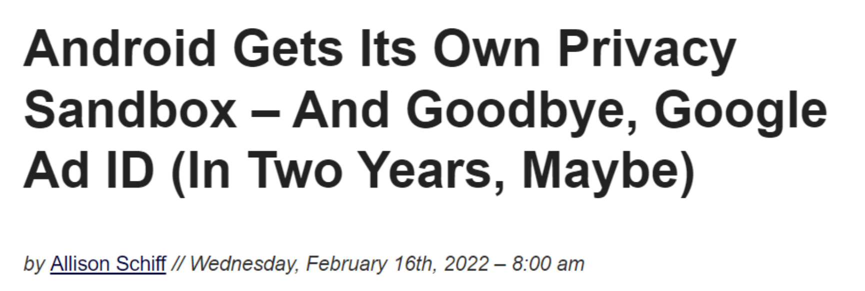
CMSC 491/691

L04 – Usable Privacy

Icons from https://thenounproject.com/

Previously on…

- Privacy Enhancing Technologies (PETs)
- Traditional vs. Emerging
    - Encryption, De-identification, Access Control
    - Homomorphic Encryption, Trusted Execution Environment, Differential Privacy, Multi-party Computation, Federated Analysis



Android Gets Its Own Privacy Sandbox – And Goodbye, Google Ad ID (In Two Years, Maybe)

by Allison Schiff // Wednesday, February 16th, 2022 – 8:00 am

In the news!

Are PETs enough?

“For the dynamic, pervasive computing environments of the future, give computing end-users ***security they can understand and privacy they can control****.”*

Computer Research Association (CRA), 2003. Four Grand Challenges in Trustworthy Computing, CRA Conference on Grand Research Challenges in Information Security and Assurance, Airlie House, Warrenton, Virginia, November 16–19, 2003.

Are just PETs enough?

“h) Psychological acceptability: It is ***essential*** *that the* ***human interface be designed for ease of use****, so that* ***users routinely and automatically apply the protection mechanisms correctly****. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use,* ***mistakes will be minimized****. If he must translate his image of his protection needs into a radically different specification language, he will make errors.”*

Jerome H. Saltzer and Michael D. Schroeder, The protection of information in computer systems, in Proceedings of the IEEE, Institute of Electrical and Electronics Engineers, Inc., 63(9), September 1975, pp.1278-1308.

Privacy Policies

- Let consumers **know about site/app’s privacy practices**
- Consumers can then **decide** whether practices are acceptable, when **to opt-in or opt-out**, and who to do business with
- Presence of privacy policies **increases consumer trust**

Users need to understand privacy policies to control their privacy

Cranor/Hong/Reiter – Usable Privacy and Security CMU 2006

Privacy Policies

- But policies are often:
  - **difficult to understand**
  - **hard to find**
  - **take a long time to read**
  - **change without notice**
- People don’t read privacy policies
- And when they do, they don’t understand them

201 hours per year on average to read policies of services we encounter! [1]

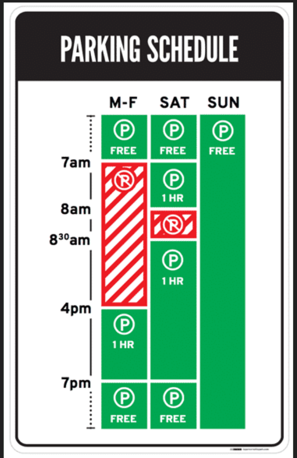
[1] Aleecia M. McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, Winter 2008-09 4(3): 543-568

Human Computer Interaction (HCI) 101

Concerned with the **design, evaluation, and implementation** of interactive computing **systems for human use** and with the study of major phenomena surrounding them.

Author/Copyright holder: Jorge Gonzalez

VS



Author/Copyright holder: Nikki Sylianteng

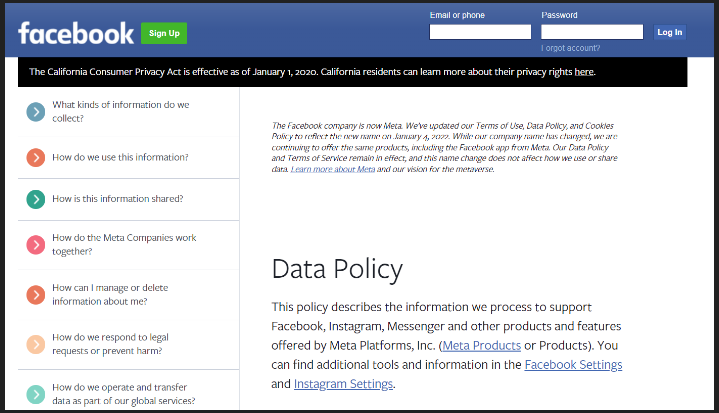
Why HCI research in privacy is critical?

- Privacy is generally **not the user’s main goal**
- **Different** groups of **users** with differing **skill sets**
- Risk of the **negative impact** of usability problems is **high**
- **Need for updates** to accommodate changes in legislation, regulation, organizational requirements, preferences...

Karat, C.-M., J. Karat, and C. Brodie, Editorial: why HCI research in privacy and security is critical now. International Journal of Human-Computer Studies, 2005. 63(1-2): p. 1-4.

Case Study: Facebook Apps

- Asked people what data they think apps can access from Facebook
- Have them read privacy policies or watch a video
- Ask again



The California Consumer Privacy Act is effective as of January 1, 2020. California residents can learn more about their privacy rights here.

- What kinds of information do we collect?
- How do we use this information?
- How is this information shared?
- How do the Meta Companies work together?
- How can I manage or delete information about me?
- How do we respond to legal requests or prevent harm?
- How do we operate and transfer data as part of our global services?

The Facebook company is now Meta. We've updated our Terms of Use, Data Policy, and Cookies Policy to reflect the new name on January 4, 2022. While our company name has changed, we are continuing to offer the same products, including the Facebook app from Meta. Our Data Policy and Terms of Service remain in effect, and this name change does not affect how we use or share data. Learn more about Meta and our vision for the metaverse.

Data Policy

This policy describes the information we process to support Facebook, Instagram, Messenger and other products and features offered by Meta Platforms, Inc. (Meta Products or Products). You can find additional tools and information in the Facebook Settings and Instagram Settings.

https://www.facebook.com/policy.php

https://takethislollipop.com/

Case Study: Facebook Apps

- Every user **underestimated what data could be accessed** when they were first asked
- Every user **improved after reading the privacy policy or watching the video**
- The **video led to greater improvements** in user understanding

- **Poor usability!**
- But **policies are really important**
- How can we **convey the information in a more usable way**?

Informed Consent

- **Users understand what data is being collected and shared and they consent to how it used**
- Components:
  - Disclosure
  - Comprehension
  - Voluntariness
  - Competence
  - Agreement
  - Minimal distraction

Usable privacy requires informed consent from users

Batya Friedman, Peyina Lin, and Jessica K. Miller. Informed consent by design. Security and Usability (2005): 495-521

How to Achieve Informed Consent?

- Many approaches have been presented!
- Sometimes fantastic ideas but **would they work in the real world?**
- We’ll look at how it started and how is it going:
    - **Platform for Privacy Preferences (P3P)**
    - **Automated analysis of privacy policies**

Platform for Privacy Preferences (P3P)

- 2002 W3C Recommendation
- **XML format for Web privacy policies**
- Protocol enables clients to locate and fetch policies from servers
- Enables development of tools that:
  - Summarize privacy policies
  - Compare policies with user preferences
  - Alert and advise users

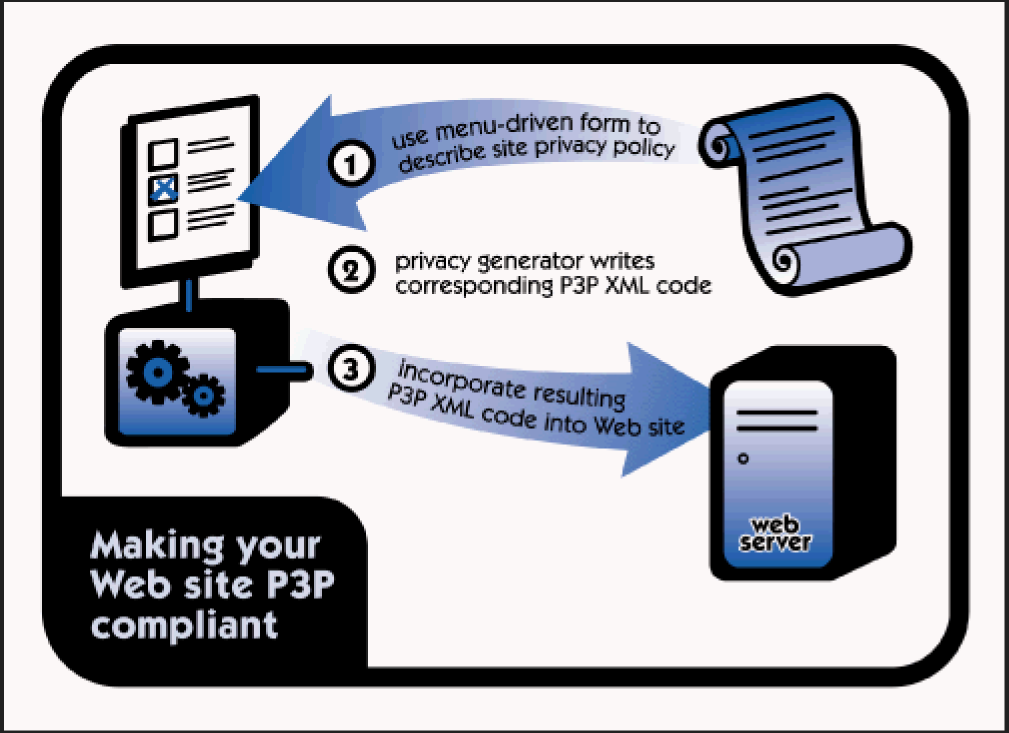
W3C® Platform for Privacy Preferences Initiative
Technology and Society domain

PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT

Enabling smarter Privacy Tools for the Web

https://www.w3.org/P3P/

How It Works

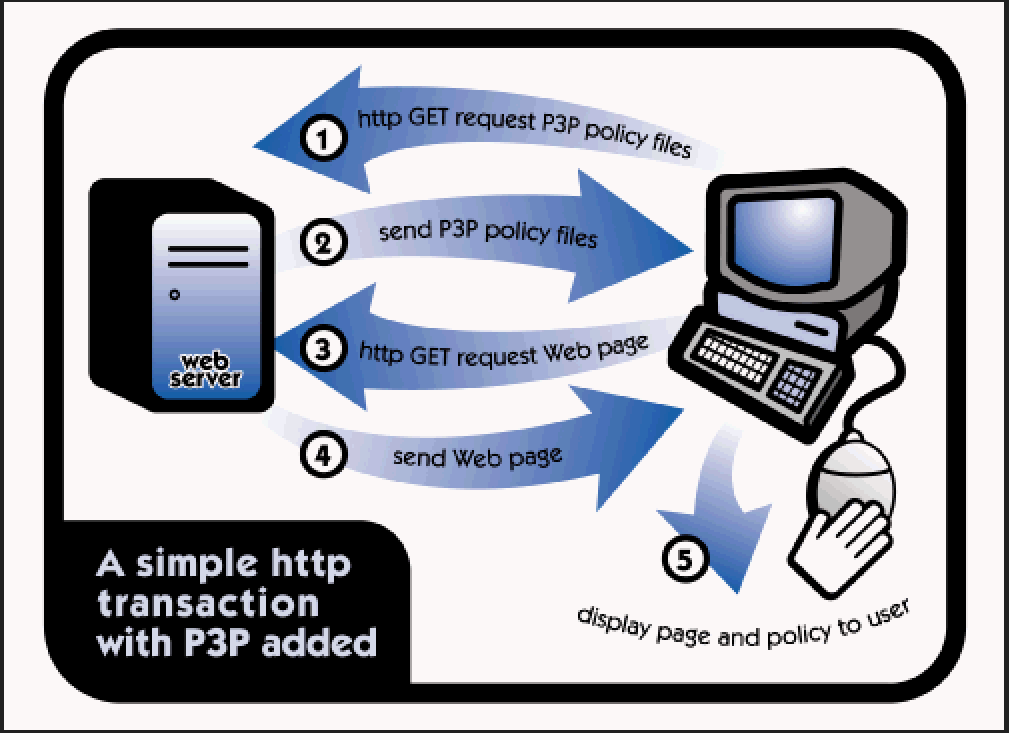


1 use menu-driven form to describe site privacy policy

2 privacy generator writes corresponding P3P XML code

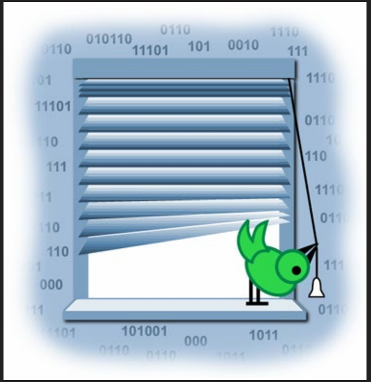
3 incorporate resulting P3P XML code into Web site

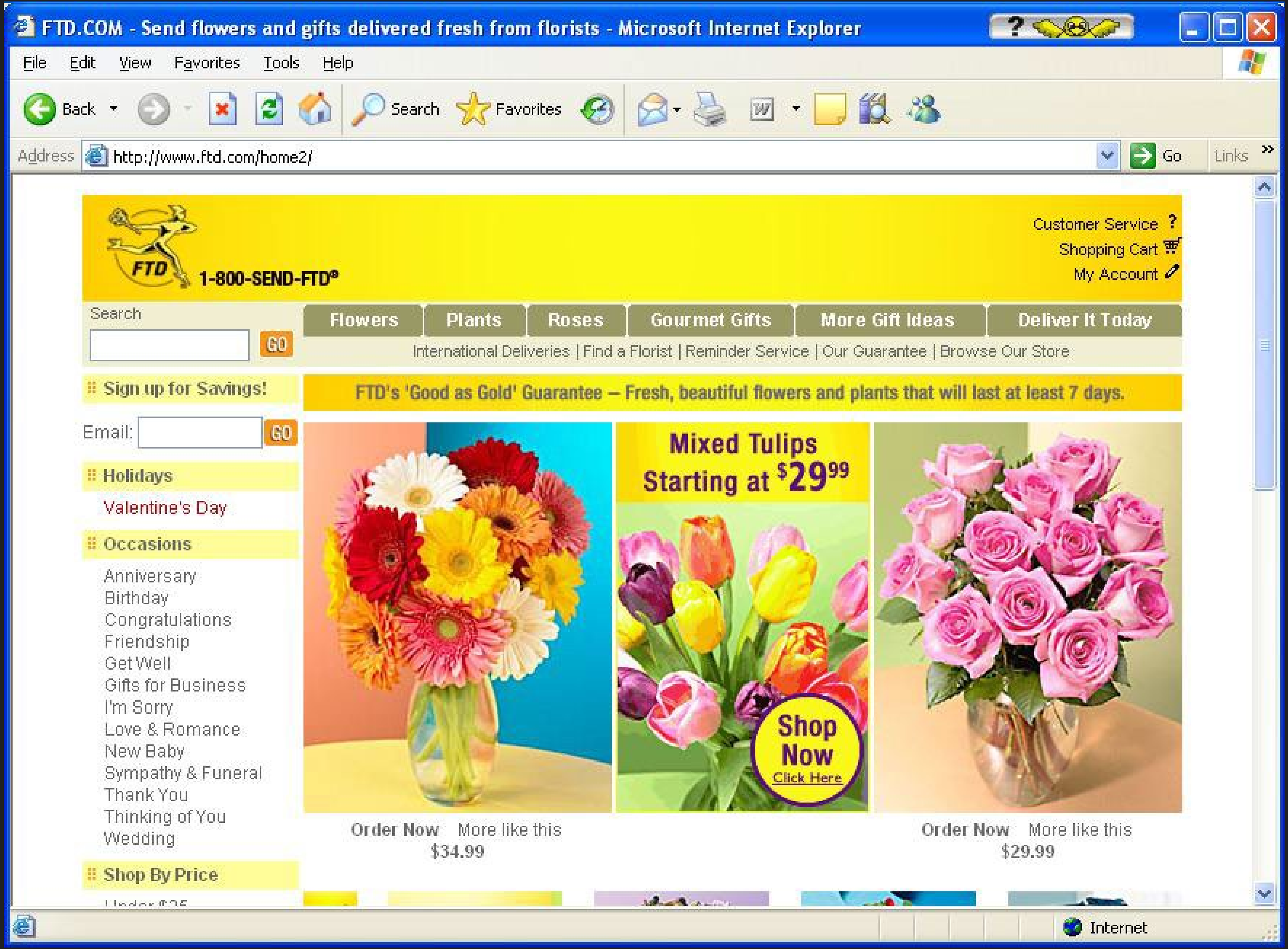
How It Works


1 http GET request P3P policy files
2 send P3P policy files
3 http GET request Web page
4 send Web page
5 display page and policy to user
web server
A simple http transaction with P3P added

Privacy Bird

- http://privacybird.com/
  - Originally developed at AT&T Labs
  - Released as open source
- “Browser helper object”
- Reads P3P policies at all P3P-enabled sites automatically
- Bird icon at top of browser window indicates whether site matches user’s privacy preferences
- Clicking on bird icon gives more information





FTD.COM - Send flowers and gifts delivered fresh from florists - Microsoft Internet Explorer

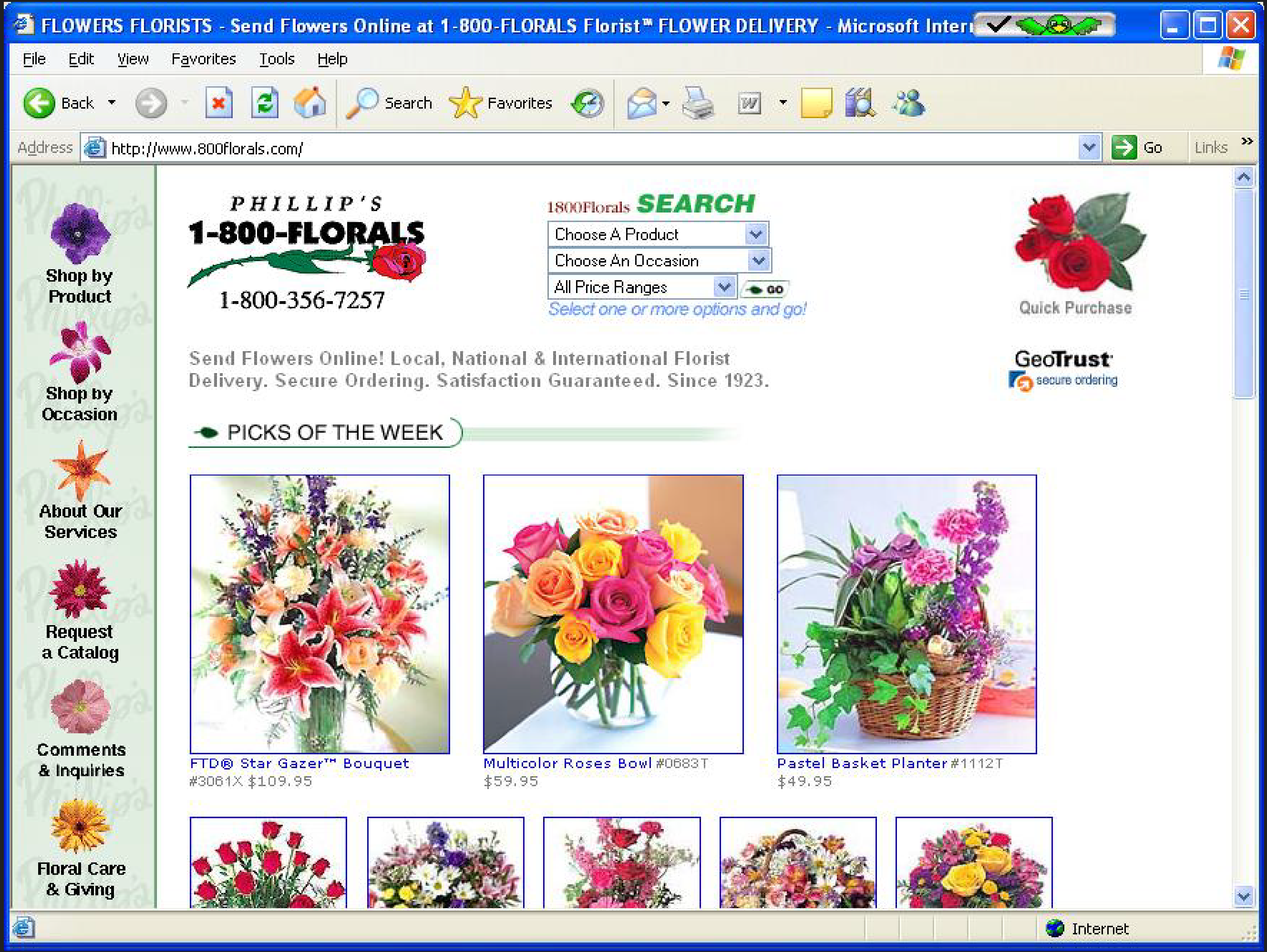
Address http://www.ftd.com/home2/

FTD's 'Good as Gold' Guarantee — Fresh, beautiful flowers and plants that will last at least 7 days.

Mixed Tulips Starting at $29.99

Order Now More like this $34.99

Order Now More like this $29.99



http://www.800florals.com/

PHILLIP'S 1-800-FLORALS 1-800-356-7257

Select one or more options and go!

Send Flowers Online! Local, National & International Florist Delivery. Secure Ordering. Satisfaction Guaranteed. Since 1923.

PICKS OF THE WEEK

FTD® Star Gazer™ Bouquet #3061X $109.95

Multicolor Roses Bowl #0683T $59.95

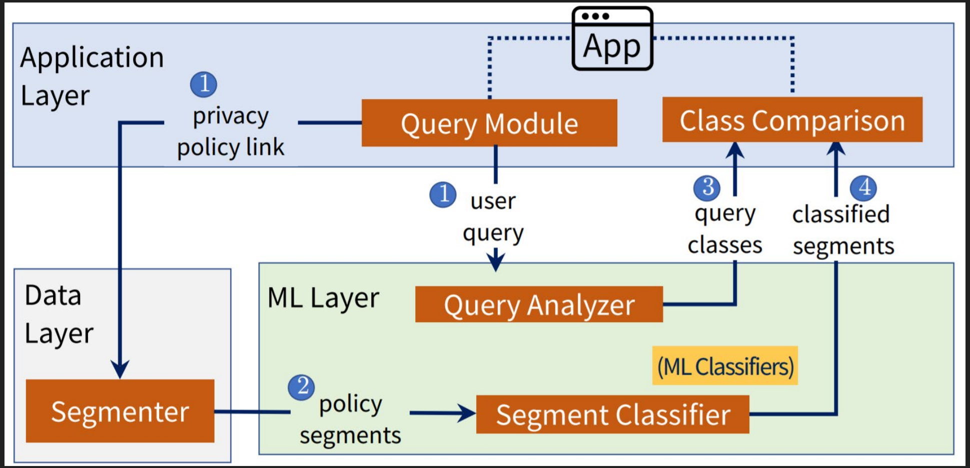
Pastel Basket Planter #1112T $49.95

What happened to P3P?

- In theory it was a good idea…
  - CDT → P3P and Privacy: An Update for the Privacy Community.
  - *“is not a panacea for privacy”* but “*does represent an important opportunity to make progress in building greater privacy protections in the Web experience of the average user.”*
- It never really picked up:
  - Few costumers:
    - Browsers: Internet Explorer/Edge (stopped support on Windows 10)
    - Websites: few websites contained P3P files
  - Lack of incentive / regulations
  - Difficult to implement
- Controversy: Does it even protect privacy?
  - See Why is P3P not a PET? and Pretty Poor Privacy

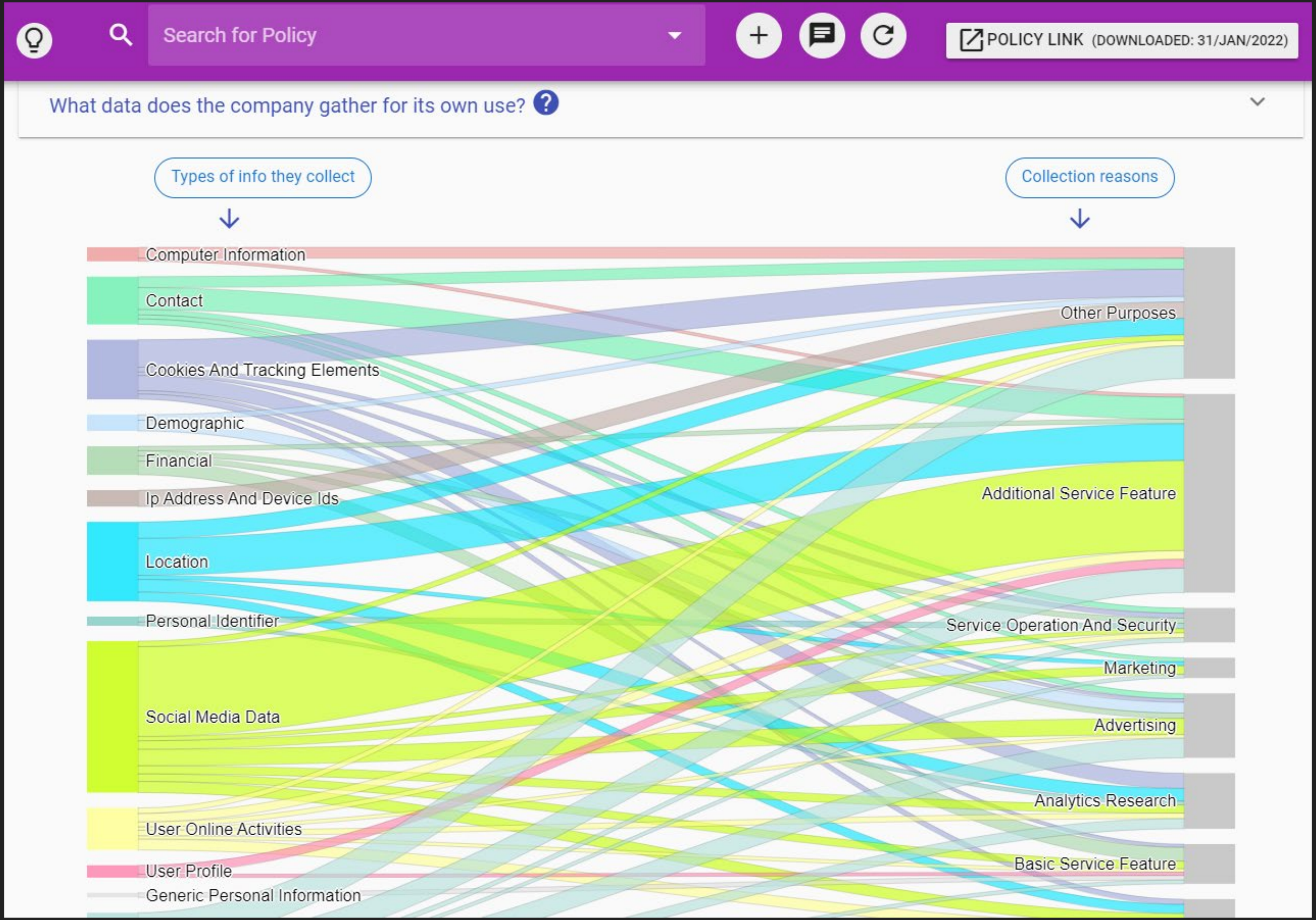
Automated Analysis of Privacy Policies

- Automatically process Privacy Policies
- Summarize and extract insights
- Present results to the user



- Example: **Polisis**
- Parse policies and generate visualizations of type of data collected, reasons, and options
- Summarize Good and Bad
- Automatically answer user questions

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., & Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. USENIX


Search for Policy
POLICY LINK (DOWNLOADED: 31/JAN/2022)
What data does the company gather for its own use? ?
Types of info they collect
Collection reasons
Computer Information
Contact
Cookies And Tracking Elements
Demographic
Financial
Ip Address And Device Ids
Location
Personal Identifier
Social Media Data
User Online Activities
User Profile
Generic Personal Information
Other Purposes
Additional Service Feature
Service Operation And Security
Marketing
Advertising
Analytics Research
Basic Service Feature

https://pribot.org/

Summary

- We need to inform users about privacy policies
- But information is not enough! Understanding is required
    - Informed consent is the goal
- It’s unfeasible to read and understand every single privacy policy
- Making decisions for users vs. Helping them make decisions

Group Activity

- Choose a service (e.g., Web application)
- Find the privacy policy
- Find this information:
    - What data they collect? for what purpose?
    - What data they share with others?
    - What are your options?