A (very lacking) tech policy primer

(Not really a primer, more a set of provocations)

Johanna Gunawan, Ph.D. Candidate

whoami

5th-year Ph.D. Candidate in Cybersecurity – Northeastern University

(adv. Dave Choffnes & Christo Wilson [NU], Woody Hartzog [BU])

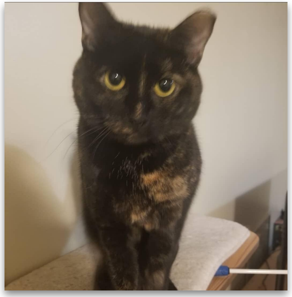
M.S., Cybersecurity 2020 | B.A., Political Science & International Affairs 2017 – Northeastern

Prior work experience in:

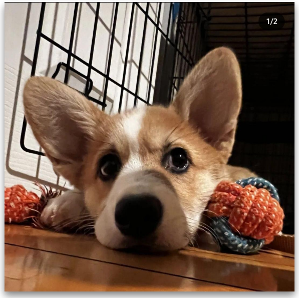
marketing software, legal & compliance in finance, technical writing & product mgmt in fintech

common sense media   vimeo   MAX-PLANCK-GESELLSCHAFT   Akamai   RAPID7

anchovy


shoyu

ebi



hodu

whoami (caveats)

Law is a big field, CS is a big field

Privacy and design regulation focus… but also theory rather than practice

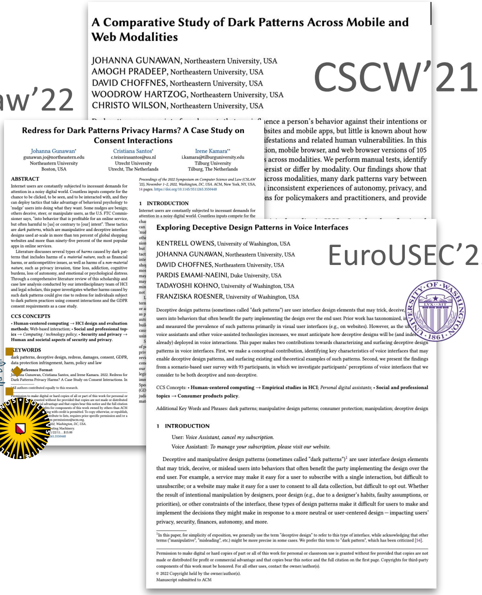
Obligatory IANAL

Dark Patterns

CSLaw'22

CSCW'21

EuroUSEC'22



A Comparative Study of Dark Patterns Across Mobile and Web Modalities

JOHANNA GUNAWAN, Northeastern University, USA
AMOGH PRADEEP, Northeastern University, USA
DAVID CHOFFNES, Northeastern University, USA
WOODROW HARTZOG, Northeastern University, USA
CHRISTO WILSON, Northeastern University, USA

…ence a person's behavior against their intentions or
…bsites and mobile apps, but little is known about how
…ifestations and related human vulnerabilities. In this
…ion, mobile browser, and web browser versions of 105
…s across modalities. We perform manual tests, identify
…ersist or differ by modality. Our findings show that
…across modalities, many dark patterns vary between
…inconsistent experiences of autonomy, privacy, and
…ns for policymakers and practitioners, and provide

Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions

Johanna Gunawan[*]
gunawan.jo@northeastern.edu
Northeastern University
Boston, USA

Cristiana Santos[*]
c.teixeirasantos@uu.nl
Utrecht University
Utrecht, The Netherlands

Irene Kamara[*]
i.kamara@tilburguniversity.edu
Tilburg University
Tilburg, The Netherlands

ABSTRACT

Internet users are constantly subjected to incessant demands for attention in a noisy digital world. Countless inputs compete for the chance to be clicked, to be seen, and to be interacted with, and they can deploy tactics that take advantage of behavioral psychology to 'nudge' users into doing what they want. Some nudges are benign; others deceive, steer, or manipulate users, as the U.S. FTC Commissioner says, "into behavior that is profitable for an online service, but often harmful to [us] or contrary to [our] intent". These tactics are *dark patterns*, which are manipulative and deceptive interface designs used at-scale in more than ten percent of global shopping websites and more than ninety-five percent of the most popular apps in online services.

Literature discusses several types of *harms* caused by dark patterns that includes harms of a *material nature*, such as financial harms, or anticompetitive issues, as well as harms of a *non-material nature*, such as privacy invasion, time loss, addiction, cognitive burdens, loss of autonomy, and emotional or psychological distress. Through a comprehensive literature review of this scholarship and case law analysis conducted by our interdisciplinary team of HCI and legal scholars, this paper investigates whether harms caused by such dark patterns could give rise to redress for individuals subject to dark pattern practices using consent interactions and the GDPR consent requirements as a case study.

CCS CONCEPTS

• **Human-centered computing → HCI design and evaluation methods**; Web-based interaction; • **Social and professional topics →** *Computing / technology policy*; • **Security and privacy → Human and societal aspects of security and privacy**.

KEYWORDS

dark patterns, deceptive design, redress, damages, consent, GDPR, data protection infringement, harm, policy and law

Reference Format:
Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions. In

[*] All authors contributed equally to this research.

Proceedings of the 2022 Symposium on Computer Science and Law (CSLAW '22), November 1–2, 2022, Washington, DC, USA. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3511265.3550448

1 INTRODUCTION

Internet users are constantly subjected to incessant demands for attention in a noisy digital world. Countless inputs compete for the

Exploring Deceptive Design Patterns in Voice Interfaces

KENTRELL OWENS, University of Washington, USA
JOHANNA GUNAWAN, Northeastern University, USA
DAVID CHOFFNES, Northeastern University, USA
PARDIS EMAMI-NAEINI, Duke University, USA
TADAYOSHI KOHNO, University of Washington, USA
FRANZISKA ROESNER, University of Washington, USA

Deceptive design patterns (sometimes called "dark patterns") are user interface design elements that may trick, deceive, … users into behaviors that often benefit the party implementing the design over the end user. Prior work has taxonomized, i… and measured the prevalence of such patterns primarily in visual user interfaces (e.g., on websites). However, as the ub… voice assistants and other voice-assisted technologies increases, we must anticipate how deceptive designs will be (and indee… already) deployed in voice interactions. This paper makes two contributions towards characterizing and surfacing deceptive design patterns in voice interfaces. First, we make a conceptual contribution, identifying key characteristics of voice interfaces that may enable deceptive design patterns, and surfacing existing and theoretical examples of such patterns. Second, we present the findings from a scenario-based user survey with 93 participants, in which we investigate participants' perceptions of voice interfaces that we consider to be both deceptive and non-deceptive.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**; *Personal digital assistants*; • **Social and professional topics → Consumer products policy**.

Additional Key Words and Phrases: dark patterns; manipulative design patterns; consumer protection; manipulation; deceptive design

1 INTRODUCTION

User: *Voice Assistant, cancel my subscription.*
Voice Assistant: *To manage your subscription, please visit our website.*

Deceptive and manipulative design patterns (sometimes called "dark patterns")[1] are user interface design elements that may trick, deceive, or mislead users into behaviors that often benefit the party implementing the design over the end user. For example, a service may make it easy for a user to subscribe with a single interaction, but difficult to unsubscribe; or a website may make it easy for a user to consent to all data collection, but difficult to opt out. Whether the result of intentional manipulation by designers, poor design (e.g., due to a designer's habits, faulty assumptions, or priorities), or other constraints of the interface, these types of design patterns make it difficult for users to make and implement the decisions they might make in response to a more neutral or user-centered design — impacting users' privacy, security, finances, autonomy, and more.

[1] In this paper, for simplicity of exposition, we generally use the term "deceptive design" to refer to this type of interface, while acknowledging that other terms ("manipulative", "misleading", etc.) might be more precise in some cases. We prefer this term to "dark pattern", which has been criticized [54].

Manuscript submitted to ACM

European Commission

OECD

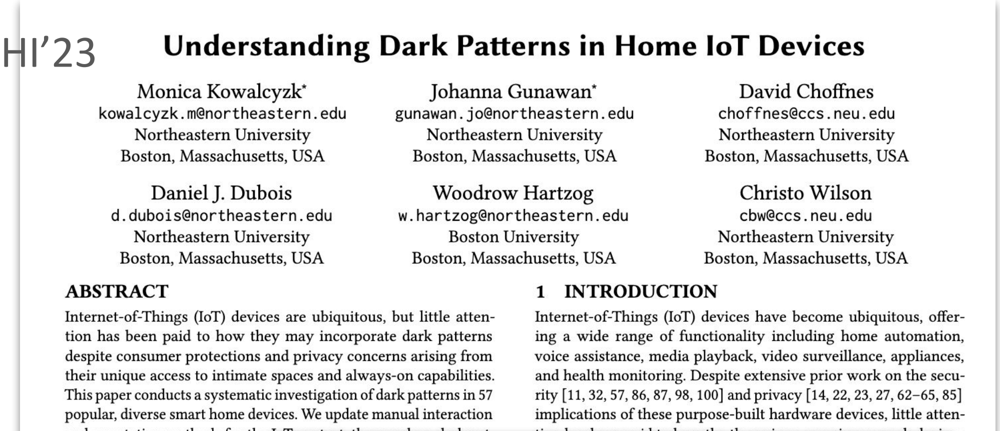
PRIVACYCON
FEDERAL TRADE COMMISSION
NOVEMBER 1, 2022

NOTHING TO HIDE?
A DATA PRIVACY PODCAST

Bringing **Dark Patterns** to **Light**
AN FTC WORKSHOP

darkpatternsresearch.slack.com

CHI'23



Understanding Dark Patterns in Home IoT Devices

Monica Kowalczyk[*]
kowalczyk.m@northeastern.edu
Northeastern University
Boston, Massachusetts, USA

Johanna Gunawan[*]
gunawan.jo@northeastern.edu
Northeastern University
Boston, Massachusetts, USA

David Choffnes
choffnes@ccs.neu.edu
Northeastern University
Boston, Massachusetts, USA

Daniel J. Dubois
d.dubois@northeastern.edu
Northeastern University
Boston, Massachusetts, USA

Woodrow Hartzog
w.hartzog@northeastern.edu
Boston University
Boston, Massachusetts, USA

Christo Wilson
cbw@ccs.neu.edu
Northeastern University
Boston, Massachusetts, USA

ABSTRACT

Internet-of-Things (IoT) devices are ubiquitous, but little attention has been paid to how they may incorporate dark patterns despite consumer protections and privacy concerns arising from their unique access to intimate spaces and always-on capabilities. This paper conducts a systematic investigation of dark patterns in 57 popular, diverse smart home devices. We update manual interaction and annotation methods for the I…
tern frequency across device ty…

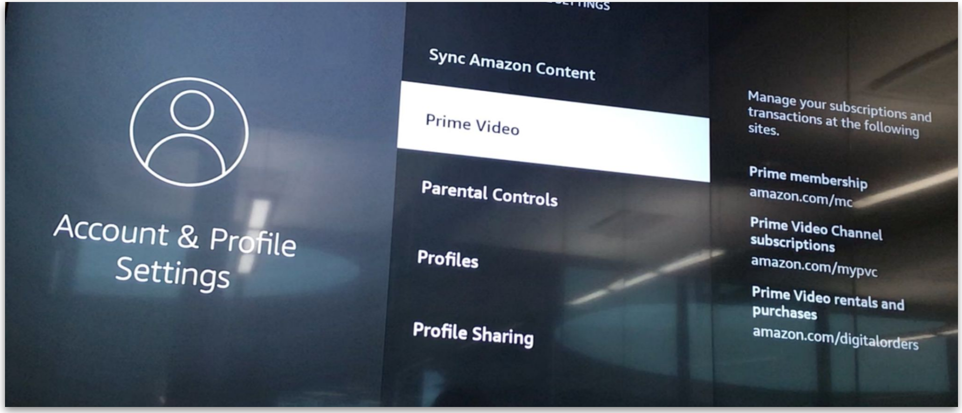
1 INTRODUCTION

Internet-of-Things (IoT) devices have become ubiquitous, offering a wide range of functionality including home automation, voice assistance, media playback, video surveillance, appliances, and health monitoring. Despite extensive prior work on the security [11, 32, 57, 86, 87, 98, 100] and privacy [14, 22, 23, 27, 62–65, 85] implications of these purpose-built hardware devices, little atten…

CR Consumer Reports

Your Smart Devices Are Trying to Manipulate You With 'Dark Patterns'

Tricky interfaces in smart speakers, internet TVs, and other devices can nudge users into giving up privacy, security, and even their money


SETTINGS
Account & Profile Settings
Sync Amazon Content
Prime Video
Parental Controls
Profiles
Profile Sharing
Manage your subscriptions and transactions at the following sites.
Prime membership
amazon.com/mc
Prime Video Channel subscriptions
amazon.com/mypvc
Prime Video rentals and purchases
amazon.com/digitalorders

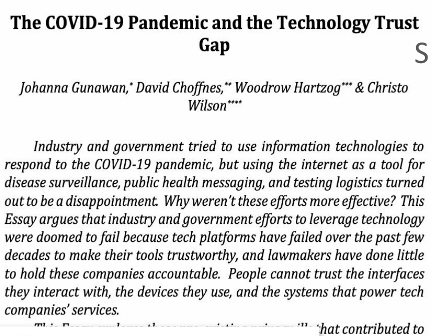
How do dark patterns differ across apps, mobile browsers, and web browsers (measurement and manual content analysis)? **Apps are major offenders**

Can dark patterns injuries eventually lead to redress and compensation claims in civil courts? **At present: potentially, with caveats and in limited cases**

What do users think about deceptive patterns in voice interfaces? **Not as problematic as hypothesized, but still of some concern**

What do we learn about dark patterns from IoT consumer electronics? **Amazon and Google (cameras/doorbells/speakers) are major offenders, but a holistic perspective is necessary**

Privacy, Surveillance, and the Law



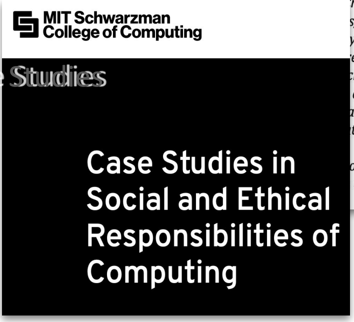
The COVID-19 Pandemic and the Technology Trust Gap

Johanna Gunawan,[*] David Choffnes,[**] Woodrow Hartzog[***] & Christo Wilson[****]

Industry and government tried to use information technologies to respond to the COVID-19 pandemic, but using the internet as a tool for disease surveillance, public health messaging, and testing logistics turned out to be a disappointment. Why weren't these efforts more effective? This Essay argues that industry and government efforts to leverage technology were doomed to fail because tech platforms have failed over the past few decades to make their tools trustworthy, and lawmakers have done little to hold these companies accountable. People cannot trust the interfaces they interact with, the devices they use, and the systems that power tech companies' services.

hat contributed to
s, consent regimes
y, and devices that
esponse is only as
chnology concerns
confidence in the
a good way to help
ties of loyalty and
of information
ollection and use
conclude that the

SHLR'21

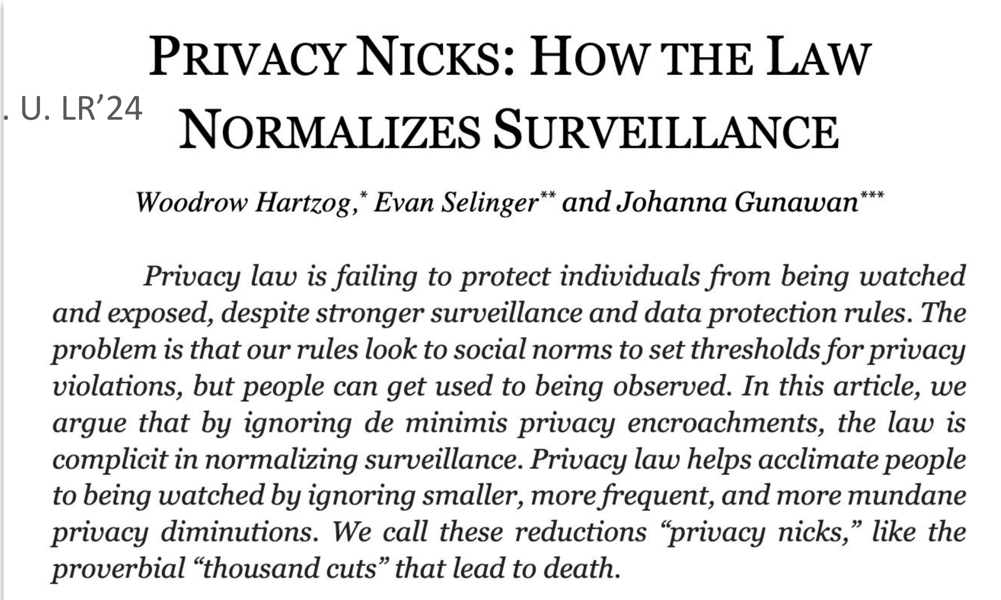


MIT Schwarzman College of Computing

Case Studies in Social and Ethical Responsibilities of Computing

SERC Case Studies '21

Wash. U. LR'24



PRIVACY NICKS: HOW THE LAW NORMALIZES SURVEILLANCE

Woodrow Hartzog,[*] Evan Selinger[**] and Johanna Gunawan[***]

Privacy law is failing to protect individuals from being watched and exposed, despite stronger surveillance and data protection rules. The problem is that our rules look to social norms to set thresholds for privacy violations, but people can get used to being observed. In this article, we argue that by ignoring de minimis privacy encroachments, the law is complicit in normalizing surveillance. Privacy law helps acclimate people to being watched by ignoring smaller, more frequent, and more mundane privacy diminutions. We call these reductions "privacy nicks," like the proverbial "thousand cuts" that lead to death.

Regulations.gov
Your Voice in Federal Decision Making

ProperData

Why does the law fail to protect us from surveillance capitalism? **The law ignores ‘death by a thousand cuts,’ which normalizes us to privacy encroachments**

Why do laypeople find it so difficult to trust emergent technologies/technological applications used in the COVID-19 public health efforts? **Trust in technology was long broken before COVID-19 uses**

Recurring themes

- *unfairness* as asymmetries in the user experience
- translating across the design stack: *knowledge sharing* between regulators/enforcers, practitioners, and researchers

‘Fairness’ under the U.S. FTC

Three-part test

- Substantial injury (caused or may cause)
- Unavoidable
- No countervailing benefits

Ongoing Work

Investigatory methods for dark patterns (w. Colin Gray, Cristiana Santos, Nataliia Bielova)

- Case law analysis of dark patterns cases across EU and US; what evidence is used for audits and what methods from scholarship is necessary for DPs enforcement? What are the regulatory gaps?
- **Early findings:** DP enforcement in the US (FTC) > enforcement in the EU, but still…

Why the law fails to regulate dark patterns - gaps & **opportunities** (w. Woody Hartzog)

- Value prioritization and jurisdictional challenges

AI and Deceptive Designs

- Currently: children's devices – emotion, voice, and facial rec in companion robots
- Trade puffery versus snake oil consumer claims? **AI featurization vs data minimization**?

Future Work

How do practitioners frame persuasive designs? (w. Yixin Zou)

- Scrape and content analysis of industry guidance/thought leadership
- Expert user study

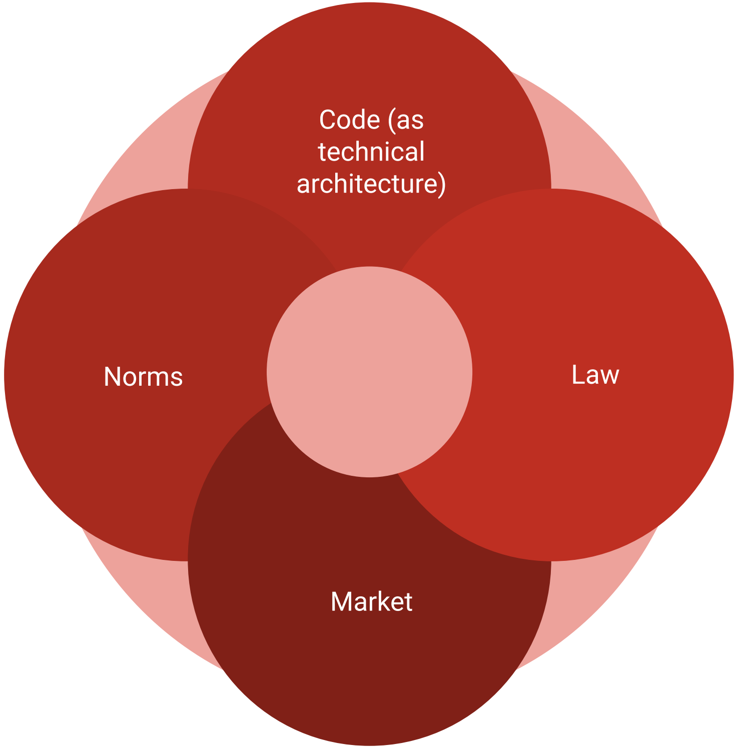
State of Auditing – towards a framework for regulators (w. Umar)

- What evidence is drawn from extant scholarship across multiple auditing types? What's been used effectively in current enforcement and what hasn't?

Modular dark patterns design study (w. Kentrell Owens, Pardis Emami-Naeini, Franziska Roesner)

- What designs do users find are more consumer/privacy protective than others?

Lessig, *The Laws of Cyberspace,* 1998



In Broad Strokes:

- Technology doesn’t originate in a vacuum, at its roots are always purposes, values, people, communities.
- Yet technology also isn’t always best understood as purely social: something special, a specific rigidity, materiality, about it.
- Technology always has effects on society, sometimes they aren’t conscious.
- Technology regulates, i.e. it shapes behavior & states of affairs.
- Technology also poses specific challenges as an object of regulation.

II. Remedy mechanisms from the GDPR

Two tier model

Two systems:

- Administrative Data Protection Authorities (DPAs) penalties framework (fines)
- **Civil law damages system in national courts (compensation for damages)**

Conditions for redress

Right to compensation (A.82 GDPR):

- Material damage(e.g. financial loss, see R.85 GDPR)
- **Non-material damage**

Conditions for compensation:

- Infringement of provisions of the GDPR
- Causal link between infringement and damages suffered

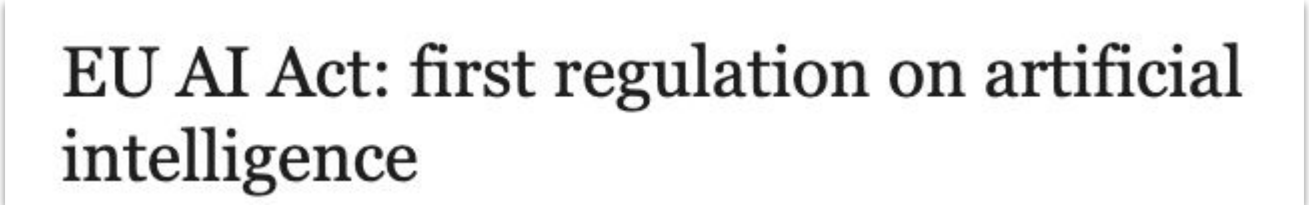
A.82 cases

Approaches for assessing damages

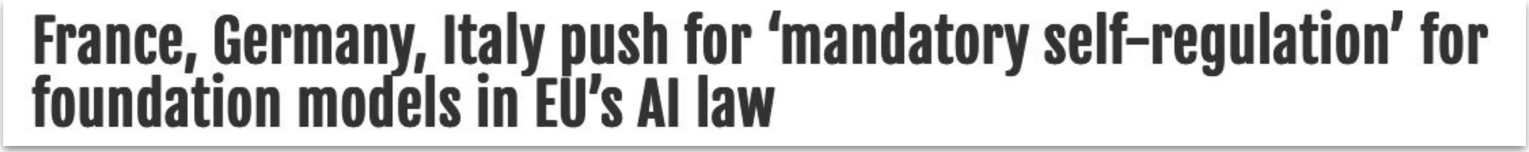
- **Infringement alone**
- **Evidentiary threshold for damages**

Nissenbaum, *Privacy in Context,* 2010

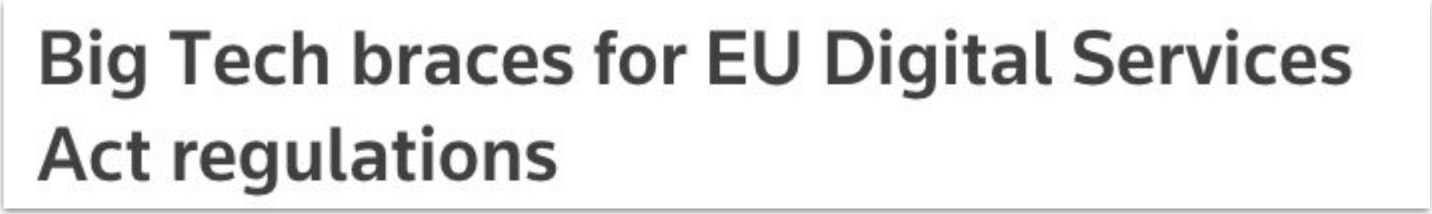
- Privacy is provided by appropriate flows of information.
- Appropriate information flows are those that conform with contextual information norms
- Contextual informational norms refer to five independent parameters: data subject, sender, recipient, information type, and transmission principle
- Conceptions of privacy are based on ethical concerns that evolve over time



EU AI Act: first regulation on artificial intelligence



France, Germany, Italy push for ‘mandatory self-regulation’ for foundation models in EU’s AI law



Big Tech braces for EU Digital Services Act regulations