May 26, 2021

(In)consistent Consent: Managing Multi-Jurisdictional Consent

Heather Federman
BigID

Ami Rodrigues
Chipotle Mexican Grill

Amanda Witt
Kilpatrick Townsend

Privacy+ Security Forum

Speaker

Privacy+ Security Forum

Heather Federman

VP of Privacy & Policy

BigID

Heather Federman is the Vice President of Privacy & Policy at BigID, where she manages and leads initiatives related to privacy evangelism, product innovation, internal compliance and industry collaboration.

Prior to BigID, Heath was the Director of Privacy & Data Risk at Macy's Inc., managing policies, programs, communications and training. Heather was also the Senior Privacy Manager at American Express Co., focusing on AMEX's global brand, marketing and digital partnerships. She previously served as a Legal & Policy Fellow for the Future of Privacy Forum and as the Public Policy Director for the Online Trust Alliance, working with companies, regulators and advocates to further FPF's mission in advancing responsible data practices and OTA's mission in establishing trust in the online ecosystem.

BigID

Speaker

Privacy + Security Forum

Ami Rodrigues

Assistant General Counsel/Privacy Officer

Chipotle Mexican Grill, Inc.

Ami Rodrigues is the Chief Privacy Officer/Data Protection Officer at Chipotle Mexican Grill, Inc. She oversees legal compliance for global privacy, cybersecurity, technology transactions, e-commerce, machine learning, and mobile app development.

Her prior experience includes working with start-ups, state government agencies, and Fortune 100 companies in setting up privacy programs, working with regulators, and navigating data security incidents. She is an adjunct professor of Privacy and Cyber Law at Georgia State University College of Law and holds the CIPP/US, CIPP/E, CIPM certifications and FIP and PLS designations from the IAPP.

Speaker

Privacy + Security Forum

Amanda Witt

Partner

Kilpatrick Townsend

Amanda Witt (@AMWitt) is a Partner in Kilpatrick Townsend's Atlanta, GA office and a co-leader of the Technology, Privacy & Cybersecurity Team. She is also a Certified Information Privacy Professional (CIPP/US and CIPP/E), as certified by IAPP.

She advises clients on the areas of U.S., EU and global privacy, cybersecurity, technology transactions, e-commerce, outsourcing, licensing and procurement, manufacturing agreements for IoT devices, intellectual property protection, strategic alliances, software and mobile app development and licensing and cloud computing. She also serves on the Executive Committee of the Privacy & Technology Section of the Georgia Bar and the Board of the International Section of the Georgia Bar.

KILPATRICK TOWNSEND

Agenda

Privacy+ Security Forum

- Challenges with Consent
- When is consent required?
- Consent Opportunities
- Is “consent” the wrong “solution”?

Challenges with Consent

Privacy+ Security Forum

Notice ≠ Consent

Privacy + Security Forum

Forbes

Privacy and Security Innovation: The Cautionary Tale of Nomi Technologies And The FTC

MAY 26, 2015 @ 11:46 AM **Tim Sparapani,** CONTRIBUTOR

Nomi, a small business formed in 2013, is a retail tracking company that gathers customer data to provide insight to traditional brick and mortar retailers about consumer traffic in their stores. In Nomi's privacy policy, the company offers consumers an opt out of Nomi's services online and at retail locations using the technology. Nomi is not required to offer consumers an opt out of this data collection because Nomi does not collect information that could identify specific customers. Nomi chose to offer these options and heeded the FTC's admonition to businesses to innovate for consumers' benefit in privacy and security practices.

The FTC brought an enforcement action against Nomi for failing to provide the promised in-store opt out. For a single misstatement, Nomi is subject to a twenty-year consent order, resulting in twenty years of government privacy audits and other compliance burdens.

NOMi

Design Failure

Privacy+ Security Forum

ars TECHNICA

GEAR & GADGETS —

Path addresses privacy controversy, but social apps remain a risk to users

Developers have quite a bit of access to users' address book data.

CESAR TORRES - 2/12/2012, 3:00 PM

We are sorry.

We made a mistake. Over the last couple of days users brought to light an issue concerning how we handle your personal information on Path, specifically the transmission and storage of your phone contacts.

theguardian

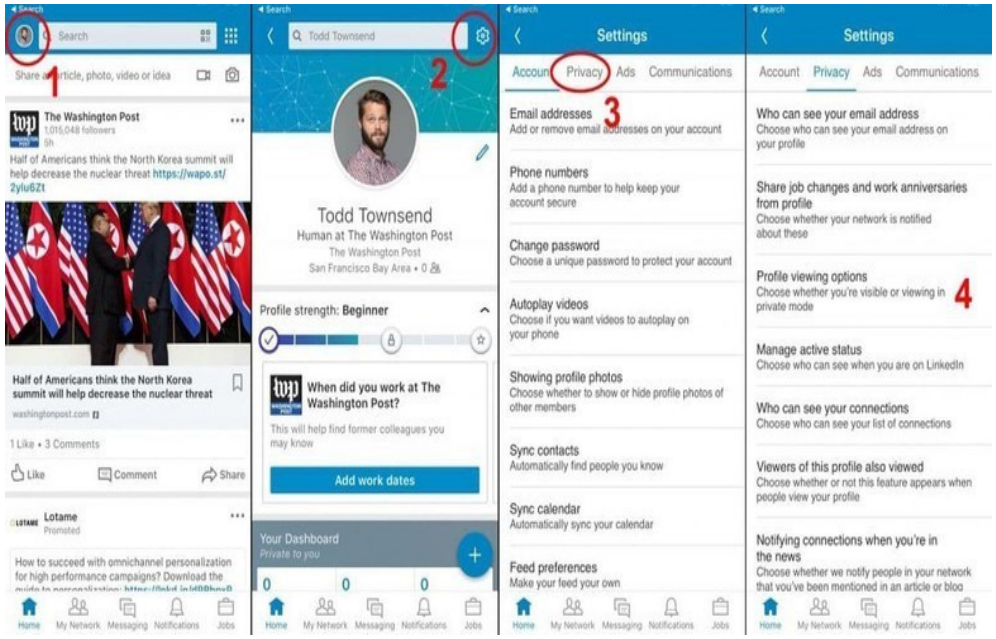
Path fined $800,000 by FTC over iOS privacy breach

Social networking app grabbed personal contact data from iPhone and iPad users and allowed children under 13 to sign up

More Choices, but less usable and more confusing?

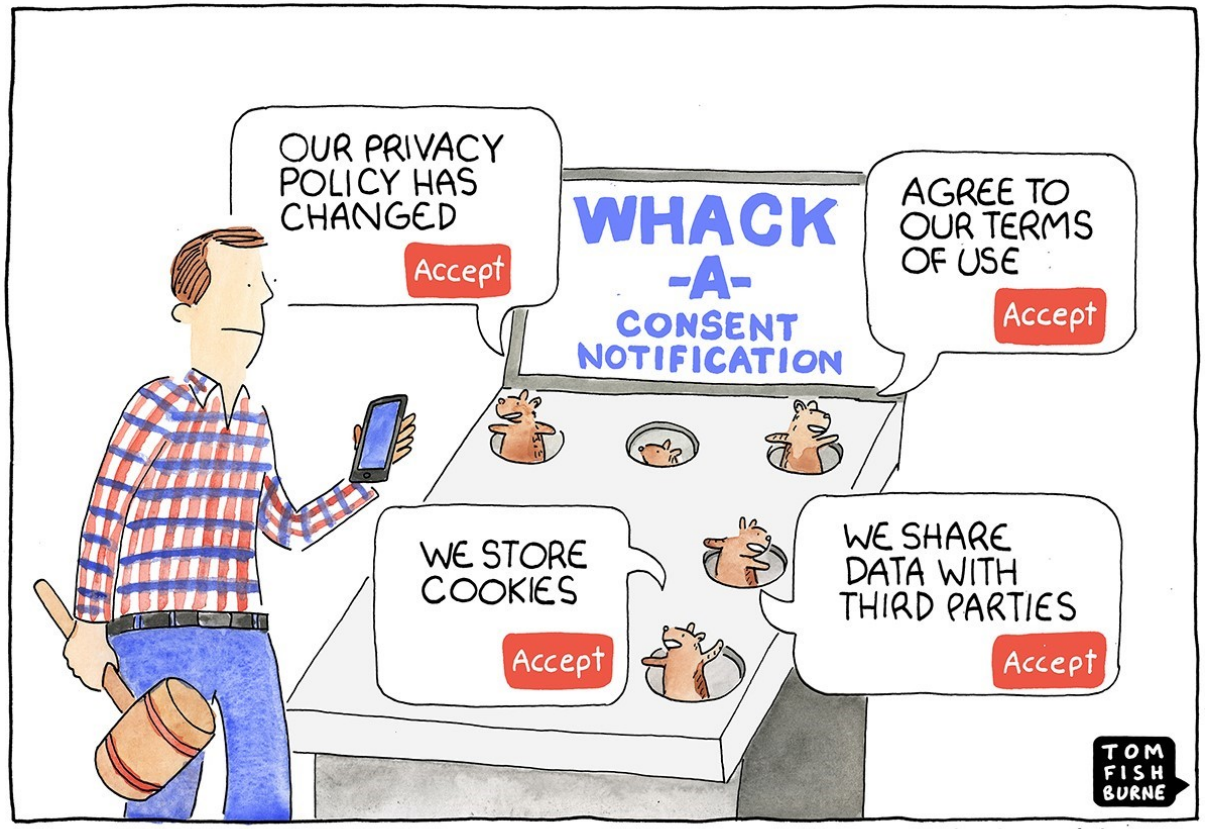
Privacy+ Security Forum

- Privacy Dashboards
- Browsers with opt-out add-ons
- Too many choices?



When Consent is Required

Privacy+ Security Forum



Sliding Scale of Consent

Privacy+ Security Forum

Implicit
Indirect, Deemed, Inferred

- Volunteered data for a clear or obvious purpose
- Acceptance inferred from actions
- Only extends to specific, immediate consent

Opt Out

- "Consent" by not declining to give consent
- Many industry guidelines (and growing # of laws) prohibit this type of consent

Opt In

- Active selection agreeing to notice

Explicit
Direct, Express, Affirmative

- Clear, documentable, unambiguous consent required for specific purpose
- Written or Verbal
- Direct Question or Data for a Purpose

Informed Consent

- Presumes forms & conditions + potential outcomes are fully understood & accepted

UK ICO Guidance on GDPR Consent

Article 4(11) of the GDPR defines consent as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

Make sure that consent:

- Is unbundled
- Includes an active opt-in
- Is granular
- Names your organization and any other controllers relying on such consent
- Is documented
- Is easy to withdraw
- Does not contain an imbalance in the relationship

CCPA on Consent

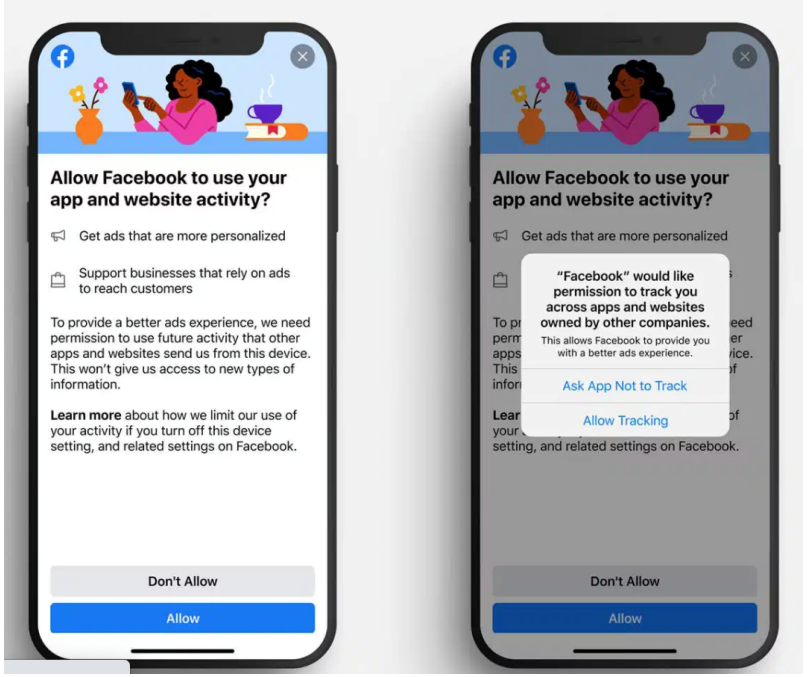
- The California Consumer Privacy Act ("CCPA") is an "opt-out" consent regime (i.e., opt-in consent is not required for adults prior to collecting or using personal information.
- Consent only arises as an issue under the CCPA for the "sale" of personal information.
- If a consumer consents or opts-in to a transfer of PI to a third party, it's not considered a "sale" under the CCPA.
- CCPA prohibits businesses from knowingly selling the PI of consumers less than 16 years of age unless the consumer (in the case of consumers b/t 13 to 16) or the guardian (for those under the age of 13) has "affirmatively authorized the sale" of PI.
- If a consumer opts out of the sale of PI, a business may not solicit such consumer's consent to a future sale for at least 12 months.

CPRA: Moving Closer to GDPR Consent

The CPRA brings California's "consent" standard closer to the strict GDPR standard in Europe. The consent standard, however, is used only in the following relatively marginal scenarios, some of which already required consent under the CCPA:

- Consenting to the sale or sharing of PI after an opt-out
- Minor opt-in consent for sale and sharing of PI
- Consenting to secondary use and disclosure of sensitive PI after an opt-out
- The research exemptions
- Opt-in consent for financial incentive programs
- Consent cannot be valid if **dark patterns** are used to obtain consent.

Industry Imposed Requirements



Optional *Required*

Consent Opportunities

Privacy+ Security Forum

Case Study

Privacy + Security Forum

- ACME Corporation is a U.S.-based global manufacturer of various goods, such as N95 masks, hand sanitizers, baking equipment, and tie-dye machinery.
- During the Great Stay of 2020, which required cities and states to go into lockdown, ACME realized it had a marketing opportunity to engage consumers across brands through its e-commerce platform.
- ACME had a Bakers & Beyond Loyalty program with ~5M members who could receive rewards and perks for purchasing baking equipment, leading to discounts and other rewards.
- **QUESTION: Can ACME share its Bakers & Beyond Loyalty program member information with other brand teams?**

Answer: It Depends 

Privacy + Security Forum

- What does the Privacy Policy for the loyalty card program say?
- More importantly, is this a type of marketing email that a loyalty consumer would reasonably expect?

Alternative Approaches

- Consider a first-party data engagement strategy that asks customers if they want to hear about deals for other brands.
- Incentivize opt-in for sharing across brands. (hint: more emails is never an incentive)
- Refresh consent where practical to ensure continued brand loyalty and engagement

Best Practices

- **Unbundled**
  - Consent is separate from T&Cs.
  - Is NOT a precondition for of signing up to a service unless *necessary* for that service.
- **Tracked**
  - Store records of consent.
  - Have the ability to connect consent with specific users or device.
  - Understand all necessary parties for a consent to be valid.
- **Customized**
  - For global consents, segment into regions and use the high bar law for such region.
  - Can also use the EU consent globally to simplify.
- **Avoided**
  - In the EU, find a legal basis other than consent if possible.

Is “consent” the wrong “solution”?

Privacy+ Security Forum

Is the Consent Framework broken?

In a well-known study at Carnegie Mellon, researchers Lorrie Faith Cranor and Aleecia McDonald determined that if every internet user were to spend eight hours per day reading every privacy policy they encountered while using the internet, it would take 76 days to complete the task.

Control is Illusory

Privacy+ Security Forum

- Privacy scholars such as Professor Woody Hartzog have identified flaws in privacy law's reliance on consent.
- Concepts such as "control", "informed consent", "transparency" and "choice" sound empowering, but notice and choice models are not scalable.
- Companies are incentivized to hide their true data practices through "manipulative design, vague abstractions, and complex words".
- Control is an illusion – interfaces are designed to extract consent
- Notice and choice regimes overwhelm users.

Questions + Contact

Heather Federman
VP of Privacy & Policy
BigID
HeatherF@bigid.com

Amanda Witt
Partner
Kilpatrick Townsend
AWitt@kilpatricktownsend.com

Ami Rodrigues
Assistant General Counsel
Chipotle Mexican Grill
ami.rodrigues@chipotle.com

Appendix

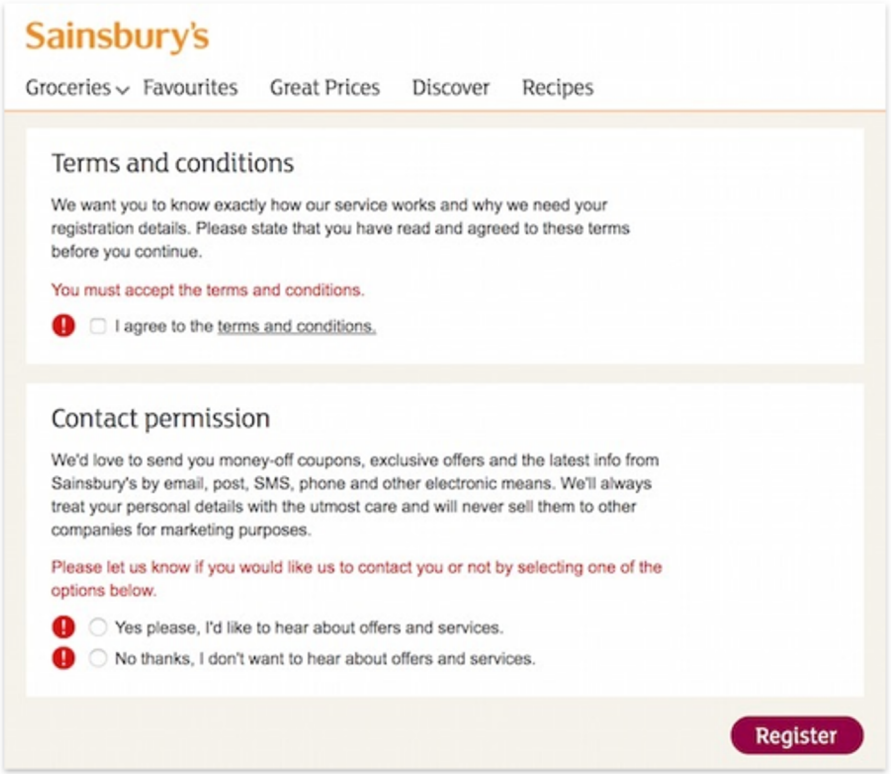
Privacy+ Security Forum

Best Practices

Privacy+ Security Forum

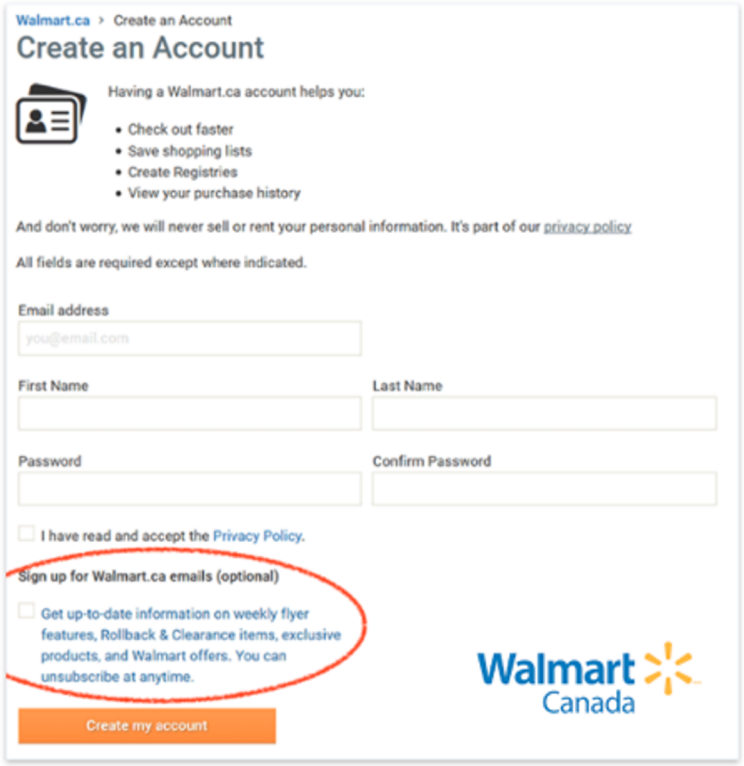
- **Unbundled**
  - Consent is separate from T&Cs.
  - Is NOT a precondition for of signing up to a service unless *necessary* for that service.
- **Active/Affirmative Opt-in**
  - Use unticked opt-in boxes or similar active opt-in methods.
  - Binary choices are given equal prominence.
- **Granular**
  - Different options to *separately* consent for different types of processing where appropriate.
- **Name Parties**
  - Name your organization and 3Ps relying on consent.
- **Easy To Withdraw**
  - Tell users they have the right to withdraw their consent at any time & how to do so.
  - Simple & effective mechanism in place.
  - It's as easy to withdraw as it was to give initial consent.

Consent Best Practices - Unbundled



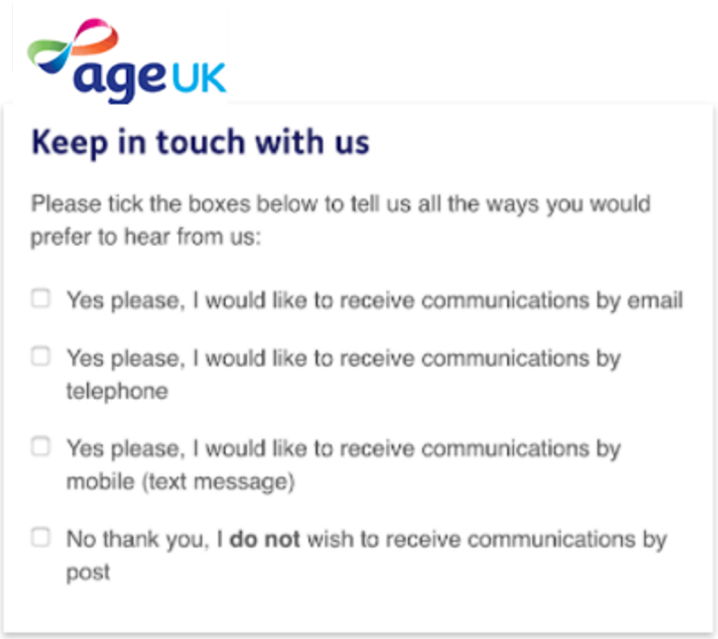
Active/Affirmative Opt In

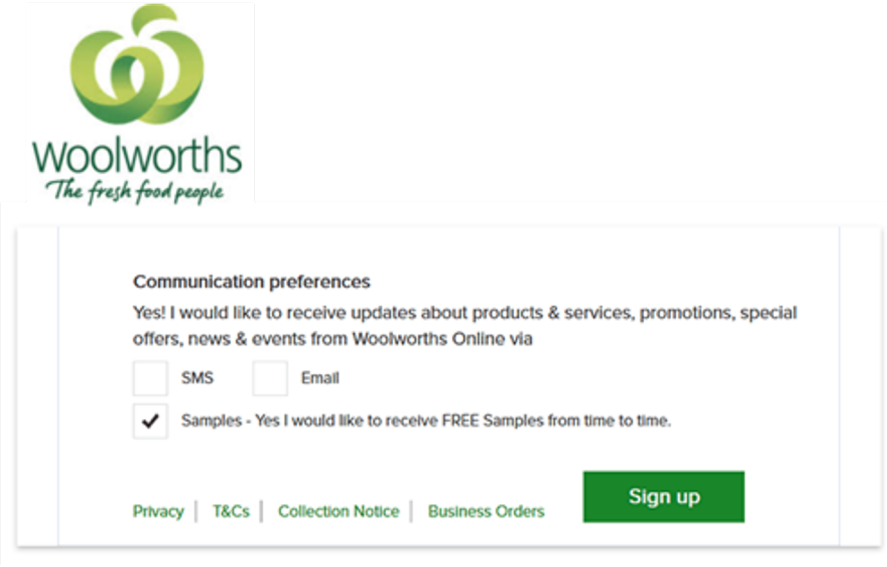
Privacy + Security Forum



Granular Consent

Privacy+ Security Forum





Named Consent

Privacy+ Security Forum

Waitrose

At Waitrose, we have exciting offers and news about our products and services that we hope you'd like to hear about. By providing your details you agree to be contacted by us*. We will treat your data with respect and you can find the details in our Contact Promise.

If you would prefer not to hear from us, you can stop receiving our updates at any time by getting in touch or by letting us know below.

- I'd prefer **not** to receive updates from Waitrose
- I'd prefer **not** to receive updates from John Lewis
- I'd prefer **not** to receive updates from John Lewis Financial Services

ageUK

We'd like to keep in touch with you about the vital work we do for older people, our fundraising appeals and opportunities to support us, as well as the products and services you can buy.

We will never sell your data and we promise to keep your details safe and secure.

You can change your mind at any time by emailing contact@ageuk.org.uk

"We", includes the charity, its charitable and trading subsidiaries, and national charities (Age Cymru, Age Scotland and Age NI).

For further details on how your data is used and stored:
www.ageuk.org.uk/help/privacy-policy

Easy to Withdraw

Privacy+ Security Forum