THE PRIVACY PRO

Privacy Audits 101

June 23, 2022

Lauren Reid

President and Principal Consultant, The Privacy Pro

The Privacy Pro helps global companies implement practical solutions to protect data, comply with laws and most importantly, respect people.

www.theprivacypro.com

@theprivacypro

Lauren Reid is President of the boutique privacy and data ethics consulting firm, The Privacy Pro. Lauren has over 15 years of global privacy experience, having worked in several countries and industries. She was the Director of Data Governance and Privacy for Sidewalk Labs, Alphabet's smart city portfolio company. She also led the National Privacy Advisory Services practice for KPMG Canada and was Senior Manager accountable for strategic privacy initiatives at Bank of Montreal, one of Canada's largest financial institutions.

Context

This presentation will discuss:

- The audit of a system, process, or product based on stated objectives, looking at evidence to see if controls are working

Not:

- An investigation to determine what went wrong
- Regulatory investigation
- Code review
- Penetration test / vulnerability scan

Why a privacy audit?

- Internal or External Audit
- Data Processor / Service Provider
  - SOC Report
  - ISO 27002/27701 Certification
  - “Right to Audit” clauses in contracts

Why a privacy audit?

GDPR/UK GDPR Article 28: Processor

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that … shall stipulate, in particular, that the processor:

   (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

GDPR/UK GDPR Article 39: Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

   (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

Why a privacy audit?

Office of the Information and Privacy Commissioner of Alberta

Office of the Privacy Commissioner of Canada

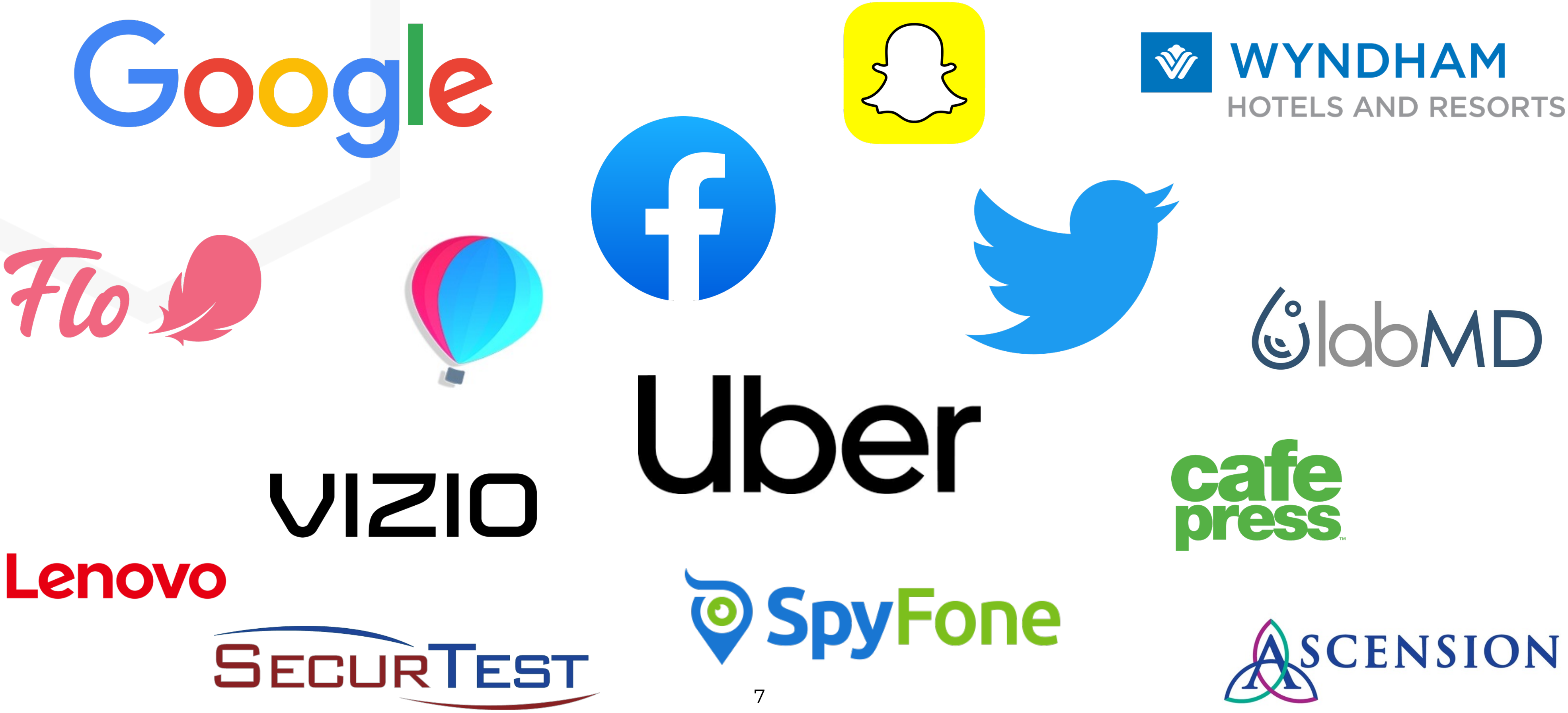
Office of the Information & Privacy Commissioner for British Columbia

Getting Accountability Right with a Privacy Management Program

2) Assess and Revise Program Controls

- The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised.
- For critical or high-risk processes, periodic internal or external audits are important ways to assess the effectiveness of an organization’s privacy program. However, at a bare minimum, the Privacy Officer should conduct periodic assessments to ensure key processes are being respected.

Why a privacy audit?



What is a privacy audit?

Do we have evidence that this thing was doing what it said it would do?

What is a privacy audit?

Do **we** have **evidence** that this thing was doing what it said it would do?

What is a privacy audit?

Do we have evidence that **this thing** was doing what it said it would do?

What is a privacy audit?

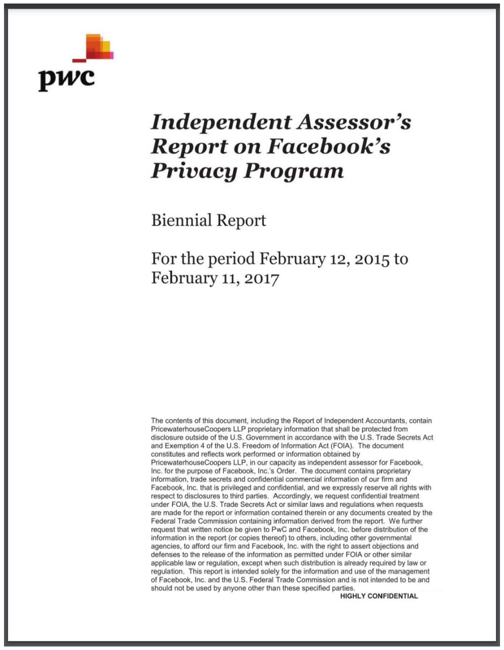
Do we have evidence that this thing **was doing** what it said it would do?

What is a privacy audit?

Do we have evidence that this thing was doing **what it said it would do**?

Example: Audit Opinion

“In our opinion, Facebook's. privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, based upon the Facebook Privacy Program set forth in Management's Assertion.”



pwc

Independent Assessor’s Report on Facebook’s Privacy Program

Biennial Report

For the period February 12, 2015 to February 11, 2017

The contents of this document, including the Report of Independent Accountants, contain PricewaterhouseCoopers LLP proprietary information that shall be protected from disclosure outside of the U.S. Government in accordance with the U.S. Trade Secrets Act and Exemption 4 of the U.S. Freedom of Information Act (FOIA). The document constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Facebook, Inc. for the purpose of Facebook, Inc.'s Order. The document contains proprietary information, trade secrets and confidential commercial information of our firm and Facebook, Inc. that is privileged and confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under FOIA, the U.S. Trade Secrets Act or similar laws and regulations when requests are made for the report or information contained therein or any documents created by the Federal Trade Commission containing information derived from the report. We further request that written notice be given to PwC and Facebook, Inc. before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Facebook, Inc. with the right to assert objections and defenses to the release of the information as permitted under FOIA or other similar applicable law or regulation, except when such distribution is already required by law or regulation. This report is intended solely for the information and use of the management of Facebook, Inc. and the U.S. Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.

HIGHLY CONFIDENTIAL

Redacted report on FTC Website

Example: Audit Opinion

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, based upon the Facebook Privacy Program set forth in Management's Assertion.

Example: Audit Opinion

In our opinion, **Facebook's privacy controls** were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, based upon the Facebook Privacy Program set forth in Management's Assertion.

Example: Audit Opinion

In our opinion, Facebook's privacy controls **were operating with sufficient effectiveness** to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, based upon the Facebook Privacy Program set forth in Management's Assertion.

Example: Audit Opinion

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness **to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017,** based upon the Facebook Privacy Program set forth in Management's Assertion.

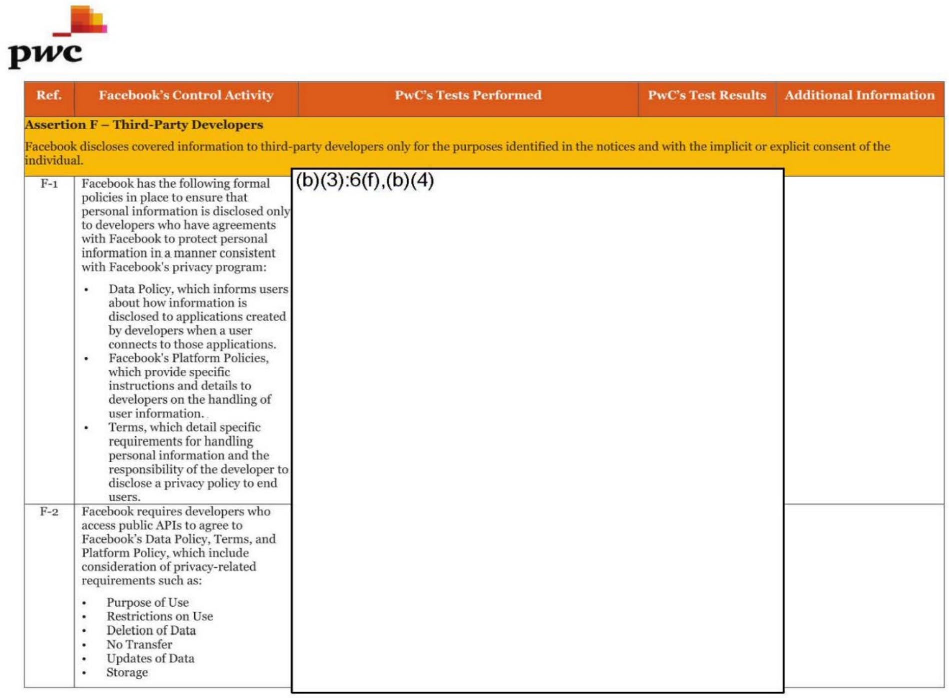
Example: Audit Opinion

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, **based upon the Facebook Privacy Program set forth in Management's Assertion.**

Example: Management Assertion

Assertion F - Third-Party Developers

"Facebook discloses covered information to third-party developers only for the purposes identified in the notices and with the implicit or explicit consent of the individual."



pwc

Ref.	Facebook's Control Activity	PwC's Tests Performed	PwC's Test Results	Additional Information
Assertion F – Third-Party Developers Facebook discloses covered information to third-party developers only for the purposes identified in the notices and with the implicit or explicit consent of the individual.				
F-1	Facebook has the following formal policies in place to ensure that personal information is disclosed only to developers who have agreements with Facebook to protect personal information in a manner consistent with Facebook's privacy program: • Data Policy, which informs users about how information is disclosed to applications created by developers when a user connects to those applications. • Facebook's Platform Policies, which provide specific instructions and details to developers on the handling of user information. • Terms, which detail specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to end users.	(b)(3):6(f),(b)(4)		
F-2	Facebook requires developers who access public APIs to agree to Facebook's Data Policy, Terms, and Platform Policy, which include consideration of privacy-related requirements such as: • Purpose of Use • Restrictions on Use • Deletion of Data • No Transfer • Updates of Data • Storage			

Example: Control Activities

- F-1) Facebook has the following **formal policies** in place to ensure that personal information is disclosed only to developers who have agreements with Facebook to protect personal information in a manner consistent with Facebook's privacy program:
    - Data Policy, which informs users about how information is disclosed to applications created by developers when a user connects to those applications.
    - Facebook's Platform Policies, which provide specific instructions and details to developers on the handling of user information.
    - Terms, which detail specific requirements for handling personal information and the responsibility of the developer to disclose a privacy policy to end users.

Example: Control Activities

- F-2/F-4) Facebook **requires developers** who access public APIs (F-2) and non-public APIs (F-4) **to agree to Facebook's Data Policy, Terms, and Platform Policy**, which include consideration of privacy-related requirements such as:
  - Purpose of Use
  - Restrictions on Use
  - Deletion of Data
  - No Transfer
  - Updates of Data
  - Storage
- (F-4) In addition, each non-public API request must be specifically approved by an authorized Facebook employee.

Example: Control Activities

- F-3) Management has implemented mechanisms to ensure that Facebook **obtains consent from users** prior to disclosing non-public personal information to third-party developers.
- **Third party developers are limited** to accessing user information based on an appropriate permission list consented to by the user.

Privacy Frameworks

AICPA Trust Services Criteria	NIST Privacy Framework	ISO 27701
AICPA American Institute of CPAs®	NIST National Institute of Standards and Technology U.S. Department of Commerce	ISO
Restructuring of Generally Accepted Privacy Principles (GAPP) Geared toward B2B (Service Organization Controls) Can certify in some contexts (SOC Reports)	Focus on privacy engineering, risk management Not specifically a privacy audit framework – but can be used as a basis for assessment	Extension of ISO 27002 (Information Security Standard) Can certify
Last updated 2017	v1.0 published in 2020	Last updated in 2019
Available from AICPA (free)	Framework and resources are open source, available on nist.gov and GitHub	Proprietary, available for purchase (~USD $185)

Illustrative* Comparison: Policies

Substantially similar objectives/controls around policies and agreements

Facebook Management Assertion	AICPA Trust Services Criteria	NIST Privacy Framework	ISO 27701
• F-1) Facebook has the following formal policies in place… • Data Policy… • Facebook's Platform Policies… • Terms…	• CC5.3) COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	• GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.	• 6.2.1.1 Policies for information security and privacy: A set of policies for information security and privacy should be defined, approved by management, published and communicated to employees and relevant external parties.

* For discussion purposes only, not a complete or authoritative mapping

Illustrative* Comparison: Agreements/Commitments

Privacy frameworks go a step further, requiring due diligence on agreements

Facebook Management Assertion	AIPCA Trust Services Criteria	NIST Privacy Framework	ISO 27701
• F-2/F-4) Facebook requires developers who access public (F-2) and non-public (F-4) APIs to agree to Facebook's Data Policy, Terms, and Platform Policy…	• P 6.4) The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. • The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.	• GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners). • GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	• A 7.2.7 Joint PII Controller: The organization shall determine respective roles and responsibilities for the processing of PII (including PII protection and security requirements) with any joint PII controller.

* For discussion purposes only, not a complete or authoritative mapping

Illustrative* Comparison: Consent

ISO, which is more closely aligned with GDPR, also requires downstream notification

Facebook Management Assertion	AICPA Trust Services Criteria	NIST Privacy Framework	ISO 27701
• F-3) Management has implemented mechanisms to ensure that Facebook obtains consent from users prior to disclosing non-public personal information to third-party developers. • Third party developers are limited to accessing user information based on an appropriate permission list consented to by the user.	• P6.1) The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.	• CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place. • CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	• A.7.2.4 Obtain and record consent: The organization shall obtain and record consent from PII principals according to the documented processes. • The organization shall inform third parties with whom PII has been shared of any modification, withdrawal or objections pertaining to the shared PII, and implement appropriate policies, procedures and/ or mechanisms to do so.

* For discussion purposes only, not a complete or authoritative mapping

Illustrative* Comparison: Records of Disclosure

All three privacy frameworks require records of disclosures

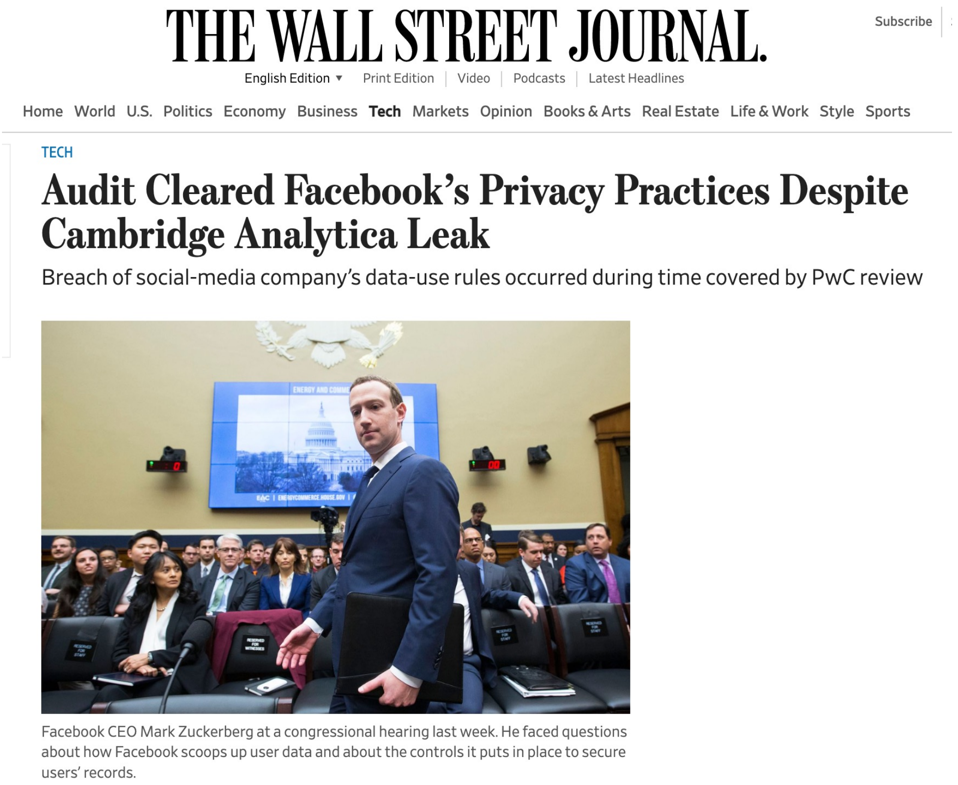
Facebook Management Assertion	Trust Services Criteria	NIST Privacy Framework	ISO 27701
• Not in scope	• P 6.2) The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.	• CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	• 7.5.4 Records of PII disclosure to third parties: The organization should record disclosures of PII to third parties, including what PII has been disclosed, to whom and at what time.

* For discussion purposes only, not a complete or authoritative mapping

Are privacy audits effective?

Do we have evidence that this thing was doing what it said it would do?

In our opinion, Facebook's privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Reporting Period, in all material respects for the two years ended February 11, 2017, based upon the Facebook Privacy Program set forth in Management's Assertion.



THE WALL STREET JOURNAL.

Subscribe

English Edition ▾ Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business **Tech** Markets Opinion Books & Arts Real Estate Life & Work Style Sports

TECH

Audit Cleared Facebook's Privacy Practices Despite Cambridge Analytica Leak

Breach of social-media company's data-use rules occurred during time covered by PwC review

Facebook CEO Mark Zuckerberg at a congressional hearing last week. He faced questions about how Facebook scoops up user data and about the controls it puts in place to secure users' records.