PRIMER ON PRIVACY

Lucy Tyson

July 12, 2017

BRACEWELL

WHAT IS PRIVACY?

Context Matters

WHAT IS PRIVACY?

- **Definition of PRIVACY from Merriam Webster Dictionary**
  - *plural* **privacies**
  - ***1a*** **:** the quality or state of being apart from company or observation **:** SECLUSION
  - ***b*** **:** freedom from unauthorized intrusion ● one's **right to *privacy***
  - ***2****archaic* **:** a place of seclusion

- https://www.merriam-webster.com/dictionary/privacy

WHAT IS PRIVACY?

- Wikipedia - Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. **The boundaries and content of what is considered private differ among cultures and individuals, but share common themes.** When something is private to a *person*, it usually means that something is inherently special or sensitive to them. **The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information.** Privacy may also take the form of bodily integrity.
- https://en.wikipedia.org/wiki/Privacy

WHAT IS PRIVACY?

- Information Collection
  - Surveillance
- Information Processing
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion
- Information Dissemination
  - Disclosure*
  - Breach of Confidentiality
  - Exposure
  - Increased Accessibility
  - Blackmail
  - Appropriation
  - Distortion
- Invasion
  - Intrusion
  - Decisional Interference

Understanding Privacy
Daniel J. Solove

WHAT IS PRIVACY?

- Privacy laws are those laws which govern the collection and use of the personal information of individuals

WHAT IS PRIVACY LAW

Speak the Language

BRACEWELL

DEFINITIONS

Personally Identifiable Information (PII), Personal Data

- Information that can alone identify an individual

Sensitive Information

- Information that is significantly related to the notion of a reasonable expectation of privacy

Non-PII

Data Subject

Data Collector

ELEMENTS COMMON TO PRIVACY LAWS

- Notice
- Choice
- Access
- Security
- Enforcement

What data is being collected?

Why is it being collected?

Can the data subject opt-out? How?

How long will it be used?

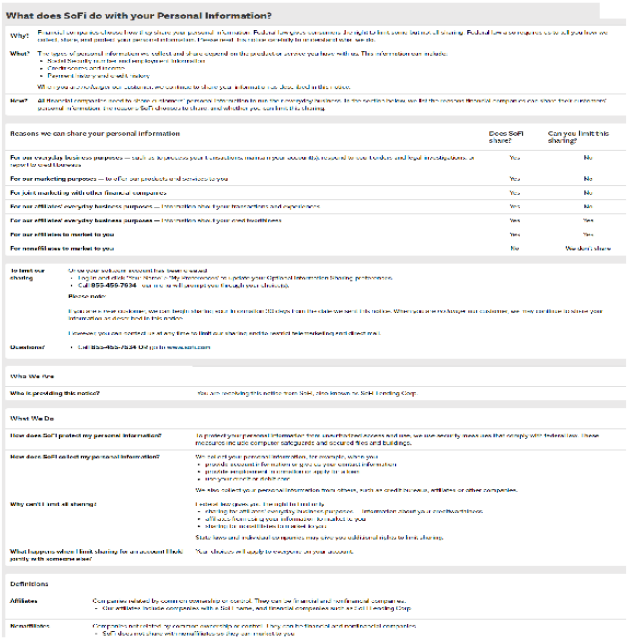
Can the data subject correct/amend?

What is done to maintain personal data?

What if a company violates the law?

NOTICE

- Provides the transparency to the data subject



What does SoFi 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 wire transfer information
- Credit history and transactions
- Payment history and credit history

We share your information as described in this notice unless you limit sharing. See below and limit sharing.

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 SoFi chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does SoFi 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	Yes	No
For our marketing purposes — to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	Yes	Yes
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share

To limit our sharing	Visit your account (if you have one) • Log in and click "Your Name > My Information" to update your Optional Information Sharing preferences. • Call 855-456-7634 and we will prompt you through your choices. Please note: If you are a new customer, we can begin sharing your information 30 days from the date we sent this notice. When you are no longer our customer, we may continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing and to cancel your marketing and direct mail.
Questions?	• Call 855-456-7634 OR go to www.sofi.com

Who We Are

Who is providing this notice?	You are receiving this notice from SoFi, also known as SoFi Lending Corp.

What We Do

How does SoFi protect my personal information?	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.
How does SoFi collect my personal information?	We collect your personal information, for example, when you • provide account information or give us your contact information • provide employment information or apply for a loan • show your driver's license We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only • sharing for affiliates' everyday business purposes – information about your creditworthiness • affiliates from using your information to market to you • sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing.
What happens when I limit sharing for an account I hold jointly with someone else?	Your choices will apply to everyone on your account.

Definitions

Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. • Our affiliates include companies with a SoFi name, and financial companies such as SoFi Lending Corp.
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. • SoFi does not share with nonaffiliates so they can market to you

BRACEWELL

CHOICE

- Opt-in
- Opt-out
- Informed Consent

CHOICE - OPT-OUT

- Consumer Credit Reporting Companies
  - Prescreened offers of credit and insurance
- Telemarketing
- Mail and Email

- www.optoutprescreen.com
- www.donotcall.gov or call 1-888-382-1222
- www.DMAchoice.org

https://www.consumer.ftc.gov/articles/0262-stopping-unsolicited-mail-phone-calls-and-email

ACCESS

- The right to view, amend, delete your data
- Limited right in some circumstances
- Right to be Forgotten
- Right to Know

Privacy ≠ Security

LAWS, WHAT LAWS?

A brief survey of the US and world

BRACEWELL

US LAWS

No generally applicable US privacy law

Tend to be industry specific or actor specific

Include federal, agency, and state regulations

- Gramm-Leach-Bliley
- Health Insurance Portability Accounting Act/HITECH Act
- Fair Credit Reporting Act (FCRA)
- Telemarketing – The Do Not Call List
- Telephone Consumer Protection Act (TCPA)
- E-Mail Marketing
- Children's Online Privacy Protection Act (COPPA)
- Privacy Act of 1974

GRAMM-LEACH-BLILEY

- Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data
- SOFI privacy notice
- Applies to:
  - Banks, brokerages, insurance companies, credit companies, mortgage companies, tax preparers, debt collectors

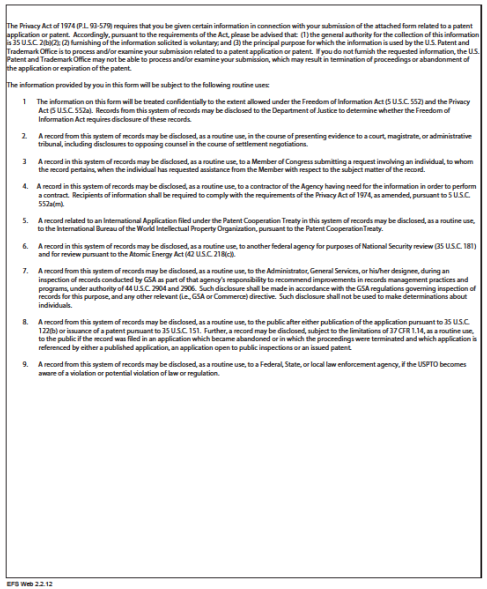
HIPAA

- Establishes national standards to protect individuals' medical records and other personal health information
- Applies to:
  - Health plans (health insurers), health care providers, health care clearinghouses, health care employee benefit plans, business associates and subcontractors (service providers, including law firms and consultants)
- Does not apply to
  - Insurance entities for life, auto
  - Fitness trackers, mobile applications
  - Wellness programs

COPPA

- Imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age

PRIVACY ACT OF 1974



Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EFS Web 2.2.12

- Can generally be characterized as an omnibus “code of fair information practices” that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies

EU LAWS

Overarching EU privacy protections

Countries can pass individual legislation

EEA countries pass legislation similar to EU

- Directive 95/46/EC (the “Directive”) – Old Law
- General Data Protection Regulation (GDPR) – New Law (Enforcement May 2018)

GDPR

- Designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.
- Applies to controllers and processors

NOTABLE DIFFERENCES BETWEEN THE DIRECTIVE AND THE GDPR

- Applicability: Applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location
- Penalties: Enhanced penalties – the greater of 4% of annual global turnover or €20 million
- Consent: Must be intelligible, using clear and plain language; withdrawal must be as easy as giving consent
- Breach Notification: mandatory notification where breach is likely to "result in a risk for the rights and freedoms of individuals"
    - Controllers notify authorities within 72 hours of becoming aware
    - Processers notify controllers "without undue delay"

NOTABLE DIFFERENCES BETWEEN THE DIRECTIVE AND THE GDPR

- Right to Access: Right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.
- Right to be Forgotten: Lots of attention in the news - entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
- Data Portability: Right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine readable format*' and have the right to transmit that data to another controller.

NOTABLE DIFFERENCES BETWEEN THE DIRECTIVE AND THE GDPR

- Privacy by Design: '*The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'.* Calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

TRANSFER OF DATA FROM EU TO THIRD COUNTRY

- Under both the Directive and the GDPR, personal data can only be transferred to countries outside the EU when an adequate level of protection is guaranteed
  - Countries deemed to have an adequate level of protection
  - Binding Corporate Rules
  - Model Clauses
  - EU-US Privacy Shield

COUNTRIES RECOGNIZED AS HAVING ADEQUATE PROTECTION

- Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay

BINDING CORPORATE RULES

- Internal rules adopted by group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection
  - European subsidiary transferring to US
  - Officially recognized under GDPR
  - Provides a global compliance solution
  - Flexibility to draft situation dependent rules
  - Available for both controllers and processors
- Process can take 18 months

MODEL CLAUSES

- Standard contractual clauses that provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights
- Standard contractual clauses for transfers from EU data controllers to data controllers outside the EU
- Standard contractual clauses for transfers from EU data controllers to processors outside the EU
  - Requires new contract with any new data transfer
  - Not considered commercially friendly (drafted by the Commission)

EU-US PRIVACY SHIELD

- Participating organizations are deemed to provide “adequate” privacy protection when transferring personal data from the European Union to the United States in support of transatlantic commerce.
  - Replaces Safe Harbor
  - Privacy Shield Framework lays out compliance requirements
  - Administered by the Department of Commerce

REST OF THE WORLD

- Argentina
- Australia
- Canada
- Colombia
- Israel
- Malaysia
- Philippines
- Singapore
- South Korea

TALKING POINTS

What is keeping you awake at night?

BRACEWELL

US PRIVACY REGULATIONS

- Current administration
  - FTC?
  - FCC?
- No overarching privacy regulation
- Big Data concerns
- Employee Privacy
  - Sensitive Information
  - Expectation of Privacy?
  - Disclosures
- State Breach Notification Laws

EU PRIVACY REGULATIONS

- Privacy Shield future is uncertain
- Regulations are complex
- Compliance can take months to a year to implement
- New role: Data Protection Officer

LAST THOUGHTS

- Publicly Available Information
  - Family Tree Now (www.familytreenow.com)
  - Spokeo (www.spokeo.com)
- LinkedIn
  - Me →Settings & Privacy → Privacy Tab (at top) → Profile Privacy → Profile viewing Options, 3 options
  - www.linkedin.com

REMOVING PUBLICLY AVAILABLE INFORMATION

- Family Tree Now
  - Go to http://www.familytreenow.com/optout
  - Read the directions and follow the steps.

- Spokeo
  - Search for yourself (see field at top of webpage)
  - Select your profile (based on name and age).
  - Visit the optout page https://www.spokeo.com/optout
  - Follow the directions

Questions?

LUCY TYSON

Associate

T: +1.713.221.3328
E: Lucy.Tyson@bracewell.com

www.bracewell.com

BRACEWELL

This presentation is provided for informational purposes only and should not be considered specific legal advice on any subject matter. You should contact your attorney to obtain advice with respect to any particular issue or problem. The content of this presentation contains general information and may not reflect current legal developments, verdicts or settlements. Use of and access to this presentation does not create an attorney-client relationship between you and Bracewell.

BRACEWELL