Website TOS vs. Your PII

Nick Johnston
nicholas.johnston@sheridancollege.ca
@nickinfosec

Introduction

Its mostly just CYA ;)

Disclaimer

I'm not a lawyer part 1: My understanding of different Terms of Service ("TOS") *may* be inaccurate but it's hopefully close enough.
I'm not a lawyer part 2: Privacy legislation is complex. The complexity increases when organizations operate in different countries. I'm leaving the finer points to the experts.

Overview

- Inspiration / previous work
- Organizational life cycle
- Categorizing data collection
- The study
- **Does your data have a life cycle?**
- What can you do?
- Questions ~~and Answers~~

Inspiration and Experience

- My former work in digital forensics:
  - Bankruptcy, receivership, and insolvency
  - Electronic discovery
  - Corporate investigations
  - Competition bureau
- NYT article June 28, 2015 - “When a Company Is Put Up for Sale, in Many Cases, Your Personal Data Is, Too”

Other people are asking this question

Ex. US bitcoin exchange Coinsetter acquires Canadian exchange Cavirtex. From Reddit:

CAVIRTEX (Coinsetter) breaks its own privacy policy. Government Honeypot? (self.Bitcoin)
submitted 3 days ago by SherlocksLatte

According to the CAVIRTEX Privacy policy https://www.cavirtex.com/privacy

"We ask for consent to collect, use or disclose client personal information, except in specific circumstances where collection, use or disclosure without consent is authorized or required by law. We may assume your consent in cases where you volunteer information for an obvious purpose."

I was not asked for my consent prior to having my information sold to a New York state company. As my information was sold as part of the database sale, I feel that I am owed my equal portion of the $2,000,000 sale amount.

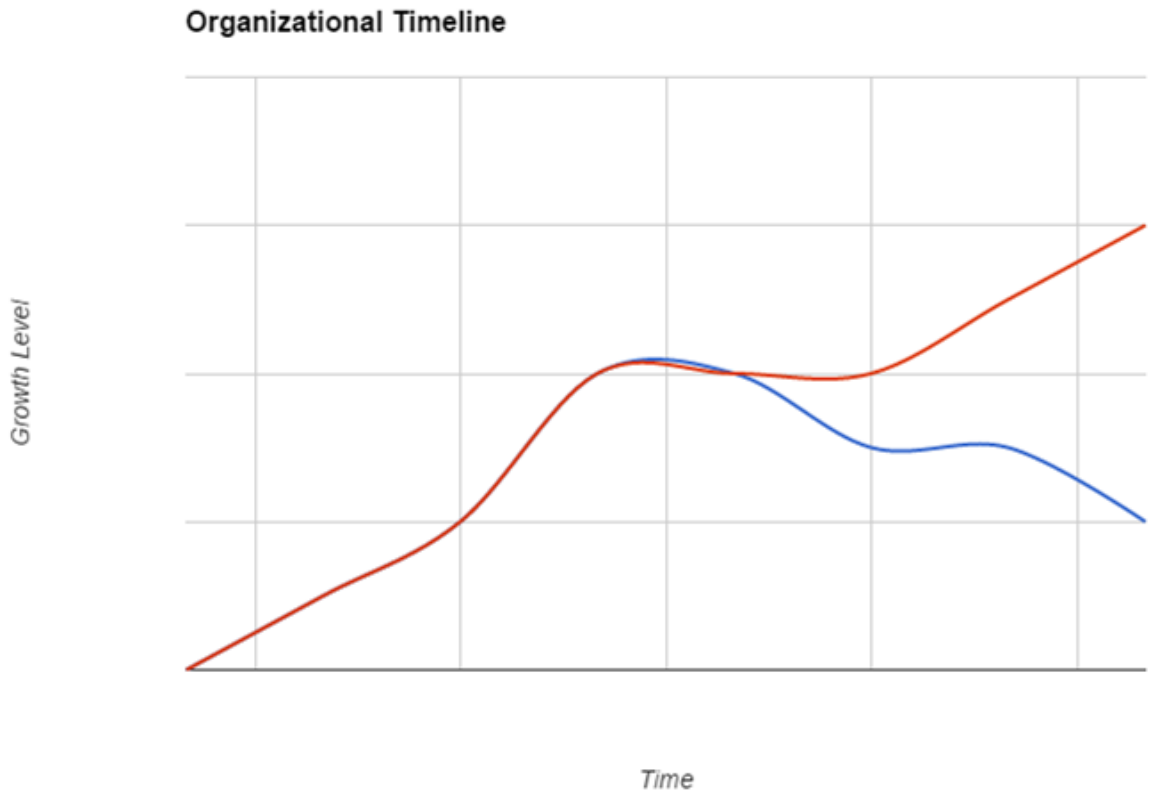
Also is my information being given to the US Government?

Some Background

Because you should know I had to make up some words

Organizational Life Cycle

1. Existence
2. Survival
3. Maturity
4. Renewal
    a. Acquisition
    b. Rebranding
5. Decline
    a. Soft close
    b. Bankruptcy



Why do orgs collect data?

- Operations
- Enhanced user experience
- Customer Relationship Management
- Sell to 3rd parties

Data Collection Categories

- Basic Identity
  - Required
  - Username, email, password
- Optional Profile
  - Optional
  - Name, Avatar, Contact Info, Likes
- Incentivized Profile
  - Same as optional profile but with incentive
  - Ex. Recommend friends / write a review for rewards

The Study

aka. The stuff I did

A Simple Survey

1. Select some websites that collect data
2. Create accounts
3. Recorded personal information fields used
4. Save the TOS
5. Examine, summarize and categorize

Note: My sampling of websites was not statistically sound and was based solely on personal interest.

Selected Websites

Adobe	Etsy	Microsoft*	Twitter
Alibaba*	Facebook*	Netflix	Wikipedia
Amazon*	Github	Nytimes	Wordpress
Apple	Google*	Paypal	Yahoo
Buzzfeed	Huffington	Pinterest	
Craigslist	Imdb	Reddit	28 Total
Dropbox	Imgur	Slack	
Ebay	Linkedin	Tumblr	

Findings by Category

Most common required fields (13-26 times)
first name, last name, username, email, *password*
Most common optional fields (10+ times)
spam/subscriptions, cc/payment, avatar picture

Not enough incentive options to justify including.

Findings by Organization

Most Required or Optional Fields (10+)
Alibaba, Amazon, Ebay, Etsy, Facebook, Github, Google, Linkedin, Microsoft, Nytimes, *Paypal*, Pinterest, Slack, Twitter, Wordpress, Yahoo - 16 Total

Most Required Fields (9-11)
Alibaba, Amazon, Google

Other finds

- Some requiring a gender selection and only listing male/female choices.
- You select the right Apple privacy policy based on your location.
- Ebay and Paypal recently split. On login, user notified of policy/privacy changes.
- 8 allow data management and/or account deletion

Findings - TOS

- **Most** organizations (all but 2) had **some** language in the privacy policy addressing “reorganization”.
- Microsoft’s privacy policy was 45 pages!
- Facebook does not appear to have a distinct privacy policy. Rolled into their “data” policy.
- 10 policies showcase their TRUSTe seal, a certification indicating strong privacy controls.

TOS Excerpts - :(

“As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but **remains subject to the promises made in any preexisting Privacy Notice** (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, **customer information will of course be one of the transferred assets**.” - **Amazon**

TOS Excerpts - :(

“[...] in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party.” - **Apple**

“Circumstances in which we may disclose user data: [...] in connection with a merger, bankruptcy, or sale/transfer of assets.” - **Craigslist**

TOS Excerpts - :(

“[...] we may choose to buy or sell assets. [...] user information, **including Personal Information, is typically one of the transferred business assets.** Moreover, if we, or substantially all of our assets, were acquired, or if we go out of business or enter bankruptcy, **user information would be one of the assets that is transferred or acquired by a third party**. [...] Following the transfer of user information in the circumstances described in this paragraph, all inquiries [...] should be directed to the entity to which the information is transferred.” - **Buzzfeed**

TOS Excerpts - Notification

“If we are involved in a reorganization, merger, acquisition or sale of our assets, **your information may be transferred as part of that deal**. **We will notify you** (for example, via a message to the email address associated with your account) **of any such deal and outline your choices in that event.**” - **Dropbox**

TOS Excerpts - Opt out

“In some cases, Etsy may choose to buy or sell assets. In these types of transactions (such as a sale, merger, liquidation, receivership or transfer of all or substantially all of Etsy’s assets), **member information is typically one of the business assets that is transferred**. If Etsy intends to transfer information about you, **Etsy will notify you** by email or by putting a prominent notice on the Site and the App, and **you will be afforded an opportunity to opt out** before information about you becomes subject to a different privacy policy.” - **Etsy**

Policy Violations Happen!

Anyway...moving along.

Organizations' Fate vs User's Data

Fate of Org

- Acquisition
- Rebranding
- Soft close
- Bankruptcy

Possible Fates of Data

- Transferred to new owner
- Remains in the company
- Fire sales
- Auctioned by appointed entity
- Assets donated / discarded
- Deleted

What can you do?

- Use anonymizing services *I2P*, Tor, VPNs, proxies and “private” browsing modes.
- Use encryption anywhere and everywhere.
- Consider “throwaway” accounts. Temporary email services are great!
- Weigh the cost/benefit of using optional or incentivised profile settings.

What can you do? (continued)

- When you stop using a site or service
  - Does the service have an account deletion feature? Can you suggest one? Just remember that it didn’t work for Ashley Madison’s users.
  - Delete the content of PII fields and maybe fill them with random data.
- Exercise your rights over your data. Treat it like you would any other personal asset.
- Read up and speak up!

Questions and Concerns

- Are users being informed of control transfer?
- Are users given options to manage their data?
- Are transfers and new uses of personal information compliant with privacy legislation?
- Are data at rest on storage media encrypted?
- Are data being wiped from discarded / auctioned / donated storage media?

References

- http://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html
- https://www.reddit.com/r/Bitcoin/comments/3gdqp0/cavirtex_coinsetter_breaks_its_own_privacy_policy/
- Lester, D., Parnell, J. and Carraher, S. (2003). Organizational life cycle: A five-stage empirical scale. International Journal of Organizational Analysis, 11(4), p.339-354.
- All the websites listed in the “Selected Websites” slide
- Personal Information Protection and Electronic Documents Act (PIPEDA) http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
- Bankruptcy and Insolvency Act http://laws-lois.justice.gc.ca/eng/acts/B-3/
- PIPEDA Case Summary #2006-336 https://www.priv.gc.ca/cf-dc/2006/336_20060621_e.asp

Website TOS vs. Your PII

Thanks for coming!

Nick Johnston
nicholas.johnston@sheridancollege.ca
@nickinfosec