To Trust or Not To Trust

What Every Startup Needs To Know About Privacy and Cybersecurity

CONNECTS Seminar at Carnegie Mellon: OCTOBER 25, 2022
John Funge, DataTribe
Drivers License Attributes on 2D Barcode by State

Biggest Data Breaches of the 21\textsuperscript{st} Century

<table>
<thead>
<tr>
<th>Rank</th>
<th>Year</th>
<th>Company</th>
<th>Records Lost (millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2020</td>
<td>CAM4</td>
<td>10,880</td>
</tr>
<tr>
<td>2</td>
<td>2017</td>
<td>Yahoo</td>
<td>3000</td>
</tr>
<tr>
<td>3</td>
<td>2018</td>
<td>Aadhaar Data Breach</td>
<td>1100</td>
</tr>
<tr>
<td>4</td>
<td>2019</td>
<td>First American Financial Corp</td>
<td>885</td>
</tr>
<tr>
<td>5</td>
<td>2019</td>
<td>Verifications.io</td>
<td>763</td>
</tr>
<tr>
<td>6</td>
<td>2021</td>
<td>LinkedIn</td>
<td>700</td>
</tr>
<tr>
<td>7</td>
<td>2019</td>
<td>Facebook</td>
<td>533</td>
</tr>
<tr>
<td>8</td>
<td>2014</td>
<td>Yahoo</td>
<td>500</td>
</tr>
<tr>
<td>9</td>
<td>2018</td>
<td>Marriott / Starwood</td>
<td>500</td>
</tr>
<tr>
<td>10</td>
<td>2016</td>
<td>AdultFriendFinder</td>
<td>412</td>
</tr>
</tbody>
</table>

Source: https://www.upguard.com/blog/biggest-data-breaches

~ 350 Major since 2004 in Wikipedia \( \rightarrow \) 20 / year
22 Million Affected by OPM Hack, Officials Say

The extent of the hack has finally been revealed.
“Mark Zuckerberg declared in 2010 that privacy is no longer a “social norm,” but bought the four houses abutting his Palo Alto home to help ensure his own privacy.”

Schneier, Bruce. *Data and Goliath*
“I believe there's an opportunity to set a new standard for private communication platforms…”

Privacy is King.
That's iPhone.
“It takes 20 years to build a reputation and five minutes to ruin it.”

Warren Buffett
What We’ll Talk About

• Big Picture
• Few Startup Axioms
• Privacy
• Security
• Questions
Big Picture
“Privacy doesn’t just depend on agency; Being able to achieve privacy is and expression of agency.”

Danah Boyd quoted in *Data and Goliath* by Bruce Schneier
So, how does this apply to startups?
Axiom 1: Focus
Axiom 2: Stage Appropriateness
Axiom 3: Find trustworthy trail guides early
Privacy
A Sea Change in the Last 5 Years

For example…

• Privacy Management Platform
• Founded 2016
• Today
  • 2,700 Employees
  • $7B valuation as of December 2021
Context

• Ever Increasing Digitalization of Life
• Cloud Computing → Democratizing Big Data
• GDPR & CCPA … and numerous others…
• AI

• No System is 100% Secure
Regulations and Trends

• There Are Many, It’s Sort of a Mess

• Some Key Regulations To Be Aware Of
  • State-level Data Breach Laws
  • General Data Protection Regulation (GDPR)
  • Fair Credit Reporting Act (FCRA)
  • Gramm-Leach-Bliley
  • Can Spam Act
  • Telephone Consumer Protection Act
  • Children’s Online Privacy Protection Act (COPPA)
  • Health Insurance Portability and Accountability Act (HIPPA)
  • Federal Election Commission

• Trends
  • National “GDPR-like” Regulation Coming to U.S.
  • California Consumer Privacy Act (CCPA)
Making Sense of It All

• Minimize what you collect
• Handle sensitive data with care
• Carefully evaluate privacy trade-offs
• Diligently protect
Key Concepts In CCPA

• Right to access
• Right to deletion
• Right to knowing if sold, and for what purpose
• Right to opt out
## US State Privacy Legislation Tracker 2022

### Comprehensive Consumer Privacy Bills

<table>
<thead>
<tr>
<th>STATE</th>
<th>LEGISLATIVE PROCESS</th>
<th>STATUTE/BILL (HYPERLINKS)</th>
<th>COMMON NAME</th>
<th>LAWS SIGNED (TO DATE)</th>
<th>CONSUMER RIGHTS</th>
<th>BUSINESS OBLIGATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Right of access</td>
<td>Right of rectification</td>
<td>Right of deletion</td>
</tr>
<tr>
<td>California</td>
<td></td>
<td>CCPA</td>
<td>California Consumer Privacy Act (2018; effective Jan. 1, 2020)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proposition 24</td>
<td>California Privacy Rights Act (2020; fully operative Jan. 1, 2023)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Colorado</td>
<td>SB 190</td>
<td></td>
<td>Colorado Privacy Act (2021; effective July 1, 2023)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>SB 6</td>
<td></td>
<td>Connecticut Data Privacy Act (2022; effective July 1, 2023)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virginia</td>
<td>SB 1392</td>
<td></td>
<td>Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Utah</td>
<td>SB 227</td>
<td></td>
<td>Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)</td>
<td>X</td>
<td>X</td>
<td>P</td>
</tr>
</tbody>
</table>

Source: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/
“Toxic Data” & Data Breach Laws

BakerHostetler
Ohio

Personal Information (i.e., “Personal Identifying Information”)
An individual’s first name or first initial with last name with one of the following identifiers:
1. Social Security number.
2. Driver’s license or identification card number.
3. Account number, credit or debit card number, in combination with and linked to any required security or access code, or password that would permit access to an individual’s financial account.

Persons Covered
Any person, including any business that is conducted in Ohio and that owns, licenses or maintains computerized data that includes personal information.

Any state agency or agency of a political subdivision.

Encryption/Notification Trigger
If the data is encrypted, redacted or altered by any method or technology in such a

https://www.bakerlaw.com/BreachNotificationLawMap
Security
A Simple Way of Breaking It Down

<table>
<thead>
<tr>
<th></th>
<th>Offense</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation-State</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Companies &amp; Criminals</td>
<td>Criminals</td>
<td>Companies</td>
</tr>
<tr>
<td>Kids in the Basement</td>
<td>✔️</td>
<td>--</td>
</tr>
</tbody>
</table>
General Guidelines

• Focus on doing the basics well

• Invest where there is risk
Top 5 Checklist
From Harvard Belfer Center Cybersecurity Campaign Playbook

1. Establish a culture of security awareness
2. Use the cloud
3. Use two-factor authentication
4. Encrypted messaging for sensitive comm.
5. Plan and prepare

Source: https://www.belfercenter.org/cyberplaybook
Improving your security is a process. You can take control. Don’t just throw your hands up.
Other Things to Keep in Mind
Third Party Risk

At Dropbox, the security of your data is our highest priority.

See why millions of people and organizations trust us with their most important work.

Protect your account.

Visit the Dropbox Trust Guide.

Security at Atlassian

Security is built into the fabric of our Cloud products, infrastructure, and processes, so you can rest assured that your data is safeguarded.

Cloud product security

Security is built into the fabric of our Cloud products. We employ numerous controls to safeguard your data including encryption in transit across our cloud services, external vulnerability research such as our Bug Bounty program, and more.

Security operations and best practices

Our dedicated security team approaches security holistically with a common controls framework. Security threats are prevented using our Atlassian Trust Management System (ATMS), secure
Customers & Partners May Hold You Accountable

- Limitation of Liability. **EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX), IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS/REPUTATIONAL HARM, REVENUE, DATA, OR USE, INCURRED BY OTHER PARTY OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.** **EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX), TOTAL LIABILITY FOR A SERVICE IS LIMITED IN ALL CASES AND IN THE AGGREGATE TO THE AMOUNT OF FEES ACTUALLY PAID BY COMPANY FOR THE CORRESPONDING SERVICE DURING THE TWELVE (12) MONTHS PRECEDING THE DATE OF THE EVENT THAT IS THE BASIS FOR THE FIRST CLAIM.**

Be Vigilant of Open Source Tools You Use

DevSecOps

Top 10
https://owasp.org/www-project-top-ten

OWASP

snyk

sonatype
Frameworks to Know About

• Just to know about...
  • For when your startup scales… not for early-stage

• NIST
  • https://www.nist.gov/cyberframework

• System and Organization Controls (SOC)
  • Part of SSAE 16 by American Institute of CPAs
  • https://www.aicpa.org/soc
Cyber Risk Insurance
Staying Up to Date

Audio
- Cyberwire Daily
- CSO Perspectives
- Cyber Law & Policy
- Caveat
- The GDPR Guy

Email
- Daily Briefing
- Week That Was
“Complexity is the worst enemy of security...”

Schneier, Bruce. *Data and Goliath*
Thank You

John Funge
DataTribe
john.funge@datatribe.com