DeleteMe 2021 PII Marketplace Report

Metrics, trends, consumer behaviors and attitudes shaping the ecosystem of online personal information
Background and methodology

DeleteMe PII metrics

- DeleteMe actively removes personally identifying information ("PII") from public databroker sites on behalf of its customers; in so doing we get an ongoing picture of public coverage these sources provide, and level of detail they have on individuals.

- DeleteMe data is aggregated and anonymized and shows only the volume of PII being found about our customers in each category tracked. Data here reflects what is typically found in public profiles available from people search sites like Intelius, Spokeo, PeopleFinder, Pipl, and other vendors.

- The absolute PII numbers cited reflect ‘our total customer sample x all metric categories x all tracked sites’. When quoting ‘amounts of PII’ online, ‘per-person averages’ are better representative of the general population than the ‘total #’ which only reflects our user-base.

Consumer survey

- From November 08-12 2021, DeleteMe conducted a survey of 1200 US consumers, aged 18-65, via Pollfish, who utilizes a verified sample of opt-in participants and delivers surveys via mobile devices. Only respondents answering all questions were included in the final data.

- The sample was 60%/40% male vs. female; respondent age breakdown was: 12% 18-24, 29% 25-34; 39% 35-44; 10% 45-54; and 10% over 55; final results were weighted by age/gender to better align to a representative US census sample.
Key findings

Industry

- The amount of online PII (represented by the sample of DeleteMe users) has grown 150% in the past 2 yrs, driven by a combination of growing level of detail included in data broker profiles, as well as more time spent online due to Covid-fueled remote work and commerce.

- Online PII has changed qualitatively over time, from basic ‘directory’-style data points, to including detail on family-networks, more information about past residences and employment, as well as emerging sources that can provide historical location-tracking or other behavioral insights.

- Availability of detailed online PII is helping drive rapid growth in consumer fraud, social-engineering ransomware attacks businesses, and new forms of targeted harassment.

Consumer

- Consumer privacy concerns are rising due to increased amount of daily life being spent online, and growing awareness of the potential for information abuse.

- Biggest worries are about over-reliance on cell-phones with weak privacy protections, growing awareness of the exploitability of account authentication processes, and daily annoyances like unsolicited robocalls.

- ‘Big Brother isn’t the problem’; respondents expressed least concern about Govt handling of PII, but express increased concern with unregulated commercial sale of personal info to 3rd parties.

- More than 50% of consumers express a demand for greater limits on how PII is collected, shared and used, as well as greater transparency about how information is already being employed.
### Key metrics about the data broker landscape

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of data brokers in the US</td>
<td>Over 230 in US</td>
</tr>
<tr>
<td>Number of data brokers globally</td>
<td>4000 worldwide</td>
</tr>
<tr>
<td>Global Industry value</td>
<td>Over $200bn</td>
</tr>
<tr>
<td># of pieces of online PII per person found by DeleteMe, 2019 vs. 2021</td>
<td>255 vs. 491</td>
</tr>
<tr>
<td>Avg # of categories of PII found per-person in 2021</td>
<td>6.7</td>
</tr>
</tbody>
</table>
Overall online PII is growing rapidly

- Driven by increased work-from-home due to Covid-19, and wider range of online interaction, 2021 was a boom-year for PII growth, expanding ~90% YoY, and 151% since the end of 2019.

- PII isn’t just expanding because of ‘more people online’, but also growth of ‘more detailed data about existing people’.

- Online profiles which used to be limited to directory-level information (e.g. ‘name, address, phone’) increasingly include personal detail about relations, spouses, past residences, employment, and other contextual detail.
Per-person PII growth driven by more coverage, more vendors

- ‘More data categories in online profiles’ has been the main driver of per-person online PII exposure.
- ‘More places to find it’ is a secondary factor; but companies in the business of reselling consumer information may face new hurdles going forward with the rollout of new state-level privacy regulations.
- Agencies like FTC and cybersecurity experts say growing levels of personal information online is driving growth in fraud, identity theft, social engineering/ransomware attacks, and espionage.
Family and relationship status data has become ubiquitous

- Certain basic categories of PII (name, address, phone, age) have long been easily accessible by consolidating information from public records.
- In the last 2 years however, data brokers have become more adept at cross-referencing family members, email addresses, cell phone numbers, either scraped from social media or leaked from data-breaches.
- Information about employment, legal/criminal history, or property ownership history is also increasingly-available, but often as part of higher-price background check services.
PII availability fuels growth in consumer fraud and social-engineering attacks

- “...Data breaches put people at risk for identity theft, financial fraud, and violations of privacy. The risk is even greater when the information is deliberately compiled and aggregated to create entire consumer portfolios, as data brokers do.” - US Senate Hearing - Data Brokers: Is Consumer Information Secure 2015

- “Threat actors use compromised PII to launch cyber-attacks in social engineering attempts via phishing emails, vishing, smishing, compromised websites, and social media scams in order to steal additional PII or financial information, access computer networks and resources, and perform additional cyber-attacks.” - NJCCIC, 2020 - Compromised PII: Facilitating Malicious Targeting and Fraudulent Activity

FTC reports of consumer fraud and identity theft incidents

Social-engineering methods drive ransomware effectiveness

DeleteMe 2021 PII Marketplace Report
Increased amount of life spent online is driving greater privacy concerns

- Covid-19 has forced millions of Americans to transition to an increasingly-online pattern of life, where business, commerce and social-life are increasingly being done remotely.

- While many working-age people have grown accustomed to being ‘always online’ as a norm of modern life, shifts in patterns among both older and younger groups (particularly those remote schooling) have increased their awareness of the potential risks of information exposure.

Have you changed your online behavior / information sharing practices since the Covid-19 pandemic began because of:

- Increased reliance in online shopping
- Increased general concerns about privacy
- Changing to remote work
- Change of job
- Concerns over access to health information
- Change to relationship status
- No change to behavior at all
Most consumers want stricter rules for PII use/sharing

- More than 50% of consumers express a demand for greater limits on how PII is collected, shared and used, as well as greater transparency about how information is already being employed.

- Feelings are more mixed about other forms of privacy regulation, reflecting the complexity of communicating data-use issues to consumers.
Most now looking for privacy features in online services

- More than half (62%) of consumers make some effort to understand the privacy features available with their online accounts, but few express faith about their functionality.

- Users of privacy-enhancing online tools (like VPNs, search engines, browsers) are growing but a significant share of users (14%) still take no active measures to limit data-exposure.
Consequences of Ubiquitous PII: the consumer view

- The most common annoyance driven by PII are robocalls and the scams which leverage information to try and execute fraud.

- More-serious risks are widely shared; credit-card fraud, online account breach/identity theft, and harassment are experienced by about a third of all people online.
Consumer concerns reflect awareness of risks of basic PII

- In recent past, consumers would tend to rate more-esoteric data as more important; recently this has flipped and more seem concerned about the potential abuse of very-basic identifying information.

- Increasing consumer use of new forms of secondary-authentication (like risks with 2-factor authentication, and relative insecurity of web-email and text platforms) may be driving awareness of risks of basic PII disclosure.
Facial recognition & location data a growing source of concern

- Growing emergence of Facial Recognition tech (either in passive public surveillance, use by law enforcement, or in device-authentication) is raising awareness of its potential for abuse.

- Vax-status or health related data, despite having far stronger regulation, tends to rank lower in consumer privacy concerns than expected.
Cell phone & workplace are greatest surveillance concerns

- Half of respondents ranked cell-phone surveillance as the most problematic source of new data-collection, considering the wealth of sensitive information it generally encompasses.
- Changing workforce monitoring tech also remains front of mind for many now employed remotely.
- While facial recognition concerned many for potential illegitimate use, consumers are less concerned in law enforcement application.
Public sector remains more-trusted as PII custodians; but with limits

- Health organizations and schools ranked lowest for concerns over information abuses (perhaps ironic, considering how often both are now subject to data breaches).

- Government agencies show both strong trust-levels as well as skepticism; possibly mixed due to concerns about increased law enforcement use of online data.

- Commercial orgs and search-engine providers perceived as least trustworthy in how they handle sensitive personal data.
Summary/Conclusions

- The last 2 years have seen record growth in both online PII availability and misuse, and growing consumer demand for better online privacy protections reflect that.

- As personal data online gets richer in content (including new categories of behavior, like location-data; or new ways of identifying people by proxy, like biometrics or behavioral fingerprinting), its potential value rises for both marketers as well as those looking steal / exploit it.

- While a number of states (CA, VA, CO) have passed comprehensive consumer privacy legislation in the last 2 years, and many more have bills in progress, at the Federal level, cybersecurity and anti-trust has been the focus, and consumer privacy measures have languished.

- More narrowly-targeted privacy legislation such as the ‘4th Amendment is Not For Sale Act’ (which would place limits on how PII can be shared between the private and public sector), and enforcing a single national ‘Opt Out’ standard (like the Global Privacy Control initiative) regulating consumer data collection, may present a simpler approach toward legislation that would beneficially affect the structure of the PII marketplace.