



Dragnet Surveillance Nation

How Data Brokers Sold Out America

January 2017

Author: James Scott (Senior Fellow – Institute for Critical Infrastructure Technology)

Contents

Introduction - Corporate Dragnet Surveillance Has Brought Adversaries “Home to Roost”	3
Information is Power	5
The Next-Generation of Hybrid Information Warfare Is Here	9
The Product is “You”	11
Americans Are Targeted More Successfully because America Lags Behind Global Privacy Initiatives ..	12
Who Are Data Brokers?	15
Problem 1: Data Brokers Operate in the Shadows	19
Where Do Brokers Acquire Data?	21
Problem 2: Fact: Data Brokers are Historically Negligent.....	29
ChoicePoint (2004, 2006).....	29
Dun & Bradstreet, LexisNexis , and Kroll Background America	30
LeapLab and Co-Defendants (2014).....	31
Experian (2011, 2015)	32
Problem 3: Collected Data Can Easily Be Leveraged to Manipulate Population Perception.....	34
Cyber Adversaries Weaponize Psychographic Data for Precision Targeted Attacks On Critical Infrastructure Executives and Organizations.....	36
Targeted Psychographic Attacks are Evolving	37
Psychographics Enable Tailored Sector Specific Attacks	43
Psychographics Facilitates Personalized Attacks Against High-Profile Individuals.....	43
Russia Continues to Masterfully Conducting Information Warfare Campaigns.....	45
China is Already Collecting Data to Manipulate Key Industries and Critical Infrastructure Executives .	46
The New War Against OPM Victims Has Begun.....	46
Conclusion - Information Warfare Leveraging Demographics and Psychographics is the New Normal	49
ICIT Contact Information.....	50
ICIT Websites & Social Media	50
Sources:.....	51

Dragnet Surveillance Nation: How Data Brokers Sold Out America

January 2017

Authors

James Scott, Sr. Fellow, ICIT

Copyright © 2017 Institute for Critical Infrastructure Technology – All Rights Reserved

Upcoming Event

Join us at the 2017 Critical Infrastructure Forum to learn about the findings in this research paper.



www.ICITForum.org

**Visit the ICIT Library to view additional
research and publications**

https://www.amazon.com/James-Scott/e/B01IPLQKSO/ref=dp_byline_cont_pop_ebooks_1

Introduction - Corporate Dragnet Surveillance Has Brought Adversaries “Home to Roost”

Modern hybrid warfare combines munitions, cyber-capabilities and information in multi-vector campaigns that, covertly or overtly, exploit or cripple critical infrastructure and that undermine the target’s public social constructs (nationalism, currency, etc.). Perhaps the most overlooked, yet devastatingly detrimental risks to our national security are data brokers who monetize Americans’ PII, PHI, etc., and the dragnet surveillance profiteers who gather that data. Health sector organizations, retailers, social media platforms, search engines, ISPs and other organizational genres conduct covert surveillance to aggregate and monetize each and every miniscule piece of consumer data. From your health records to credit card purchases, to your online activity, their product is “You” and monetizing your life is the exclusive business model. Most claim to remove PII from the records before each sale, but with modern data mining,

Figure 1: Script Kiddies and More Sophisticated Threats Exchange American Databases on Deep Web Markets

↑ 2 ↓

i have access to huge database of peoples info how can i profit from it?
submitted 4 months ago by Roccie

sup guys im new to all this but i believe i have access to alot of records and personal info as well as major hospital servers.... can someone help me out and point me in the right direction on how to profit from it?

Reply Subscribe Report

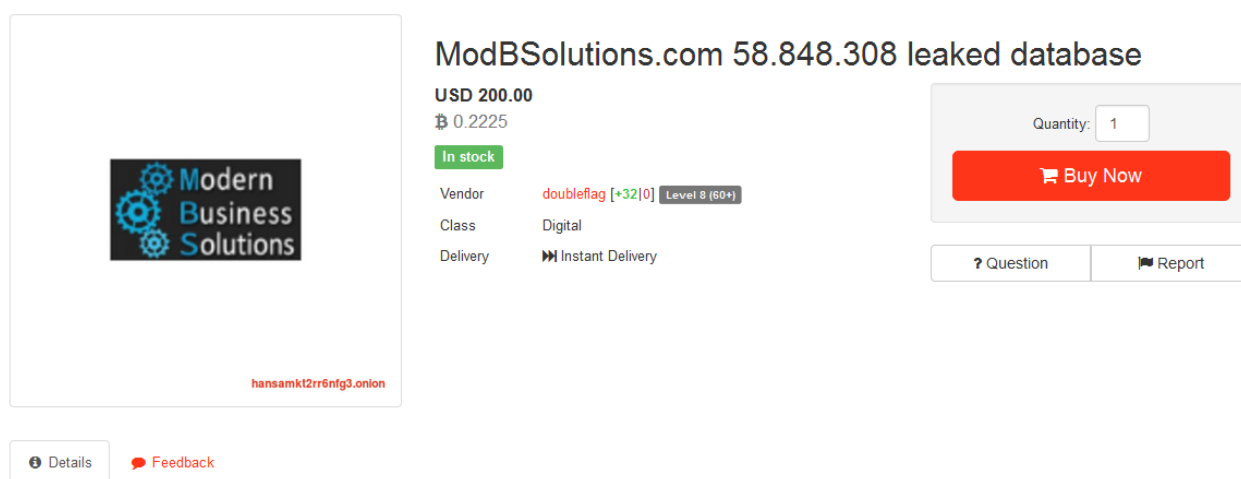
↑ Toramerica123 [Vendor] [10] 2 points 4 months ago
↓ hit me up
Reply Report

↑ gameofnumbers [Vendor] [40] 2 points 4 months ago
↓ Feel free to give a shout in PM, even if others don't see value sometimes we know what to do.
Reply Report

Dragnet Surveillance and improperly secured sensitive databases containing Americans’ demographic and psychographic information are already being bought and sold on Deep Web markets and forums by unsophisticated threat actors. They mostly employ the information in various forms of fraud. Worse, cyber-mercenaries, Advanced Persistent Threats (APTs), and other sophisticated actors are leveraging this data in more harmful attacks and in cascading breaches against critical infrastructure personnel and systems.

Big Data analytics, and abundant data sets (courtesy of mass corporate dragnet surveillance) security by anonymization is a laughable defense. Alternately, cyber-adversaries (who have backdoors and beach-heads on countless corporate networks) may pilfer the treasure troves of data from the originator network before the company anonymizes the data. The most devastating impact derives from the cascading cyber-attacks that result from the adversarial employment of the exfiltrated pseudo-anonymous or de-anonymized data in psychographic data analytics algorithms capable of creating hyper-precision targeted lures, which can be directed at high-profile individuals, critical infrastructure personnel, and the general population.

Figure 2: Alphabay Sale of Compromised Modern Business Solutions Data Aggregation Platform Information



ModBSolutions.com 58.848.308 leaked database

USD 200.00
₿ 0.2225

In stock

Vendor: **doubleflag** [+32|0] Level 8 (60+)

Class: Digital

Delivery: Instant Delivery

Quantity: 1

Buy Now

? Question Report

hansamk12rr6nfg3.onion

Details Feedback

Listing Details

58,848,308 ModBSolutions.com no passwords Business 2016-10
contains field
"email","gender","zip","state","city","address","last_name","first_name","updatedate","job"

According to its site, Modern Business Solutions is “A full service data management platform that allows you to collect, store, and transfer data records easily regardless of format type.” Figure 2 is a screenshot of a leaked ModbSolutions database listed on the Deep Web market Alphabay. The dragnet surveillance information stolen can be used in personalized attacks or to create precision focused convincing lures that appeal to targets’ psychology and behaviors.

This new war extends past the doorstep of every American. You are served to any and every adversary on a silver platter by the very service providers you use on a daily basis. Now, thanks to virtually zero regulations over this murky industry, the chickens have come home to roost. Your data is being used against you for highly customized spear phishing, malvertising, drive-by-download and information warfare initiatives. Real news, fake news, legitimate sites and spoofed websites, phishing emails, poisoned product updates and patches and more are now expertly crafted for precision targeting and mass proliferation, in digital information-warfare attack campaigns that are redefining the hybrid warfare landscape.

Information is Power

A few words, the simple fragment of an idea, can topple a nation if embedded into the right minds. Questions like “Doesn’t [public figure] look tired?”, “Is [elected official] qualified?”, or “Are [population subgroup] infringing on basic rights?” act as triggers to catalyze polarized conversations capable of rapidly destabilizing a nation or undermining its societal structure. Modern trends in private sector dragnet surveillance and recent innovations in Big Data analytics enable cyber adversaries to ascertain the societal and niche-community triggers and exploitable behavioral patterns that can be leveraged to manipulate even a cybersecurity conscious and cyber-hygienic high-value target into opening a personalized malicious lure and thereby compromising associated critical infrastructure networks.

For years, businesses have been haphazardly collecting Americans’ data through every imaginable form of dragnet surveillance. They intended to ascertain the most effective communication channels and delivery mechanisms for convincing consumers to alter their behaviors to corporate desired outcomes. Data accumulation was not cyber-hygienically limited to the collection of only necessary data; instead, entire business models were based on the collection and monetization of as much consumer data as possible. Further, this data has not been protected according to its potential or its value. As a result, data broker information sets and niche-community data sources are high-value, low-security targets for cyber-adversaries intent on launching precision focused propaganda, disinformation, malvertising, or social engineering campaigns that target individuals or critical infrastructure organizations.

Once upon a time, separating a digital record, such as an electronic health record (EHR) into name, address, social security number, etc. or deleting fields altogether, would have anonymized the data subject; however, modern easy-to-use data mining tools can cross-reference multiple databases containing anonymized and non-anonymized data, to re-identify individuals based on their information fragments. By law, any information, such as PHI, sold to data brokers must be anonymized through the separation of fields such as name, social security number, etc. However, data broker organizations often label profiles with unique numerical identifiers that can be used to re-aggregate the disparate fields back into the original de-anonymized profile. The identifier facilitates Big Data mining to build a profile, even if they do not know the data subject’s name and it makes the information more valuable [1]. Cyber adversaries can exploit these individual profiles in targeted attacks or they can leverage demographic and psychographic Big Data algorithms to target entire niche communities within critical infrastructure and within the general population.

Figure 3: Hansa Market Sale of Maryland State “Fullz”

MARYLAND state FULLZ

Vendor philobeto13 (3168) (4.83★)
Price ฿0.00349 (\$2.99)
Ships to Worldwide
Ships from CANADA
Escrow Yes



Product description

FIRST:LAST:ADDRESS:CITY:STATE:ZIP:MAIL:DOB:IP:SSN:PHONE:BANK: sometimes comes with ROUTING_NUMBER

The “fullz” sold in the Hansa Market listing depicted in Figure 3 are valuable to cybercriminals for identity theft. Big Data analytics conducted on massive databases of these “fullz” can provide adversaries with demographic and psychographic predictive information and insights that can be used in targeted attacks against the general public and against critical infrastructure systems and personnel.

Demographics (data analytics based on user attributes) and Psychographics (data analytics based on user behaviors) are employed in hyper-focused campaigns that target critical infrastructure organizations and government entities according to the psychology and quintessential life patterns of their executive and administrative personnel. It has always been true, that the “right message” attached to the proper malicious payload can give any adversary carte blanche access to any level of even the most well-protected networks. Now, adversaries have the tools and the data required to always discern the most effective and most compelling lure to coerce specific target users, operating on vital systems, into subliminally ignoring cyber-hygiene controls and into voluntarily bypassing cybersecurity defenses. Real news and fake news, legitimate websites and spoofed websites, real emails and spear phishing emails, and malvertising, collectively render endless variations of potential attacks by any adversary that enlists the precision targeting provided by psychographic and demographic data analytic tools. Private sector dragnet surveillance on users and customers enables organizations to sell data to Big Data analytics organizations that focus on tailoring marketing and promotion campaigns to population subsections, by exploiting trends in the personal interests, buying habits, political affiliation, lifestyle choices, values and passions, etc. of a specific niche audience. Adversaries can conduct demographic and psychographic analysis on the data obtained from previous breaches such as OPM, Anthem, and a constantly growing plethora of others, in order to target critical infrastructure personnel and systems.

Figure 4: American Marketing Database for Sale on Hansa Market

USA Marketing Data 79,639,498 alot of fields

USD 300.00
₹ 0.3465

In stock

Shipping options

Free all World send mail whit link to Download [Next Day] [+]

Quantity: 1

Buy Now

? Question Report

Vendor: **doubleflag** [+32|0] Level 6 (50+)

Class: Digital

Details Feedback

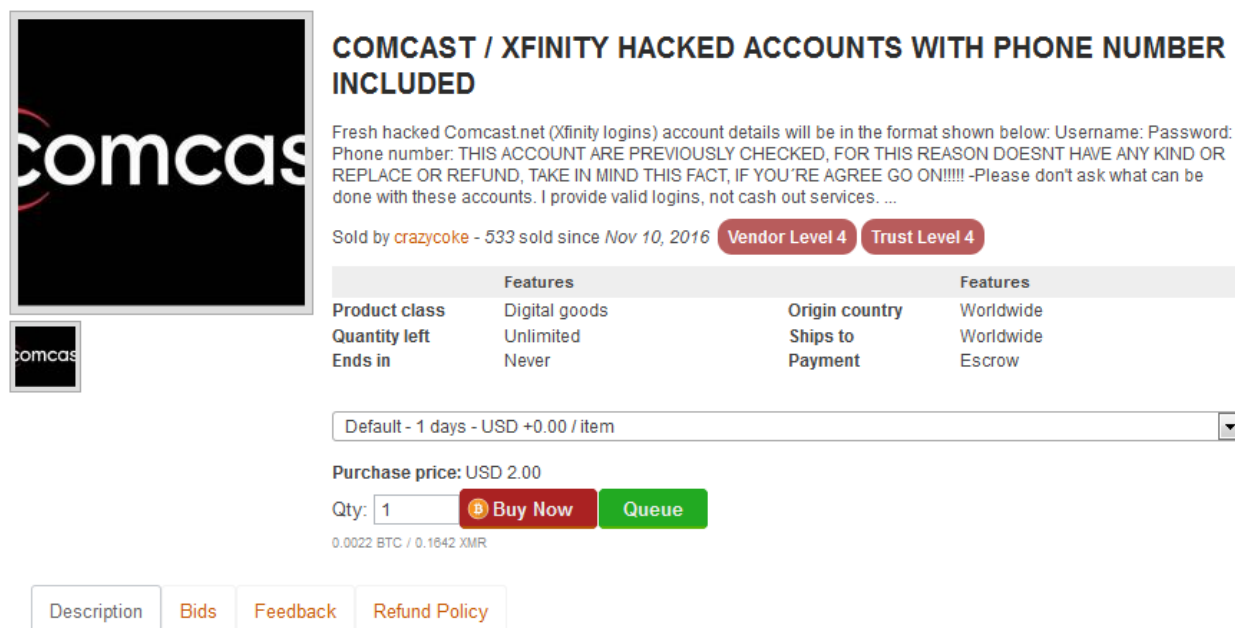
Listing Details

79,639,498 USA Marketing Data no passwords Marketing 2013

Exfiltrated Marketing databases, such as the Hansa Market listing shown in Figure 4, provide adversaries with target lists, behavior trends, etc. that facilitate unsophisticated and sophisticated precision targeted campaigns. Data Brokers, who collect and sell this information, have failed to protect this data according to its value.

Privacy advocacy has been so distracted by the concept of pinpointing National Security surveillance, by the NSA and other government bodies, that the most pronounced problem of dragnet surveillance, the organizations who collect user data and the data brokers who resell user data, have been totally ignored and permitted to operate without oversight commensurate to the modern threat landscape. Commercial dragnet surveillance operates in the name of profiteering and little else. Every individual's ISP, credit card information, health records, online purchases, free email account usage, mobile GPS usage information, etc. is sold to any and every organization wishing to overtly, covertly, or maliciously, steer societal and individual perceptions toward desired outcomes. Unfortunately, that end-state is typically to persuade the target to click on a link that redirects to a website that delivers a malicious payload that puts critical infrastructure, private sector IP, and government secrets under adversarial control.

Figure 5: Deep Web Exchange of Consumer Telecommunication Profile Information



COMCAST / XFINITY HACKED ACCOUNTS WITH PHONE NUMBER INCLUDED

Fresh hacked Comcast.net (Xfinity logins) account details will be in the format shown below: Username: Password: Phone number. THIS ACCOUNT ARE PREVIOUSLY CHECKED, FOR THIS REASON DOESNT HAVE ANY KIND OR REPLACE OR REFUND, TAKE IN MIND THIS FACT, IF YOU'RE AGREE GO ON!!!!!! -Please don't ask what can be done with these accounts. I provide valid logins, not cash out services. ...

Sold by **crazycoke** - 533 sold since Nov 10, 2016 **Vendor Level 4** **Trust Level 4**

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty: **Buy Now** **Queue**

0.0022 BTC / 0.1642 XMR

Description Bids Feedback Refund Policy

Product Description

Fresh hacked Comcast.net (Xfinity logins) account details will be in the format shown below:

Username:
Password:
Phone number:

Figure 5 depicts an Alphabay sale of Comcast account information. Consumers do not realize that everyday businesses collect massive amounts of PII or that those organizations fail to adequately secure those data from cybercriminals and more sophisticated adversaries. From these credentials, an adversary could access account profile information and assemble their own database of customers, which can be leveraged in targeted attacks. For instance, a precision lure might be to these specific Comcast users based on their watching habits and interests.

The information curated and monetized by America's private sector is being weaponized against average people for the most intricate, detailed, and precise information warfare and critical infrastructure cyberattack strategies the world has ever seen. For years, privacy advocates have warned that processes exist to de-anonymize data in order to identify and target niche-communities or specific individuals. What if an adversary could take all these benign data points and run them through Big Data analytics algorithms in order to gain insight into the most intimate passions, habits, fears, aspirations and motivations of, for instance, nationwide health sector CISOs or energy sector SCADA engineers? What if the adversaries could use this information to mirror the targets online activity to the extent that they could predict upon which content targets would carelessly click; even to the point where the target's attention or perceptions could be steered in one direction or another? The target's personal universe becomes a construct of artificially concocted fractions of reality where truths and untruths dissolve into oblivion, with the only consistency being the profound possibility of a malicious payload positioned behind each and every link.

The Next-Generation of Hybrid Information Warfare Is Here

Big Data Analytics operations on Psychographic and Demographic data are the next generation of hybrid warfare weapons. This new mechanism of hyper targeting critical infrastructure and government executives along tailored personal attack vectors streamlines the delivery of malicious code to privileged users; thereby, granting adversaries unrestricted access to most, if not all, IP, PII, EHR and other sensitive data and controls. Psychographics, and other big data analytics, provide adversaries the information needed to expedite the delivery of malicious payloads obfuscated within malicious advertisements, news and fake news, legitimate websites and spoofed websites, and real emails and spear phishing emails. These compromised data streams offer adversaries the insight necessary to target even the most cyber-hygienically advanced executives and to compromise even the most secure systems. When combined with foreign propaganda and perception management efforts, the weaponization of psychographics and demographics, facilitated by the lack of sufficient data collection and aggregation limitations, is the most innovative and the most bleeding-edge form of hybrid warfare. As more data are negligently collected and monetized with the release of each new technology, each new piece of software, and each new version of the "Terms and Conditions", this new hybrid cyberattack vector will continue to increase the leverage and influence that nation-state and mercenary cyber-adversaries can exploit to the detriment of American critical infrastructure and National Security.

Figure 6: Adversaries can Access Consumer Geolocation, Demographic, and Payment Information

UBER ACCOUNT - User and Password (Can't guarantee any CC on file or papyal or if account has a balance)

I will send the USER and PASSWORD if it stops working just pm me and Ill replace it! WILL REPLACE ONLY IF USER OR PASSWORD IS NOT WORKING I CAN NOT GUARANTEE THE THE ACCOUNT WILL HAVE A CC ON FILE OR PAYPAL OR IF IT HAS A BALANCE, WILL NOT REPLACE THE ACCOUNT UNLESS USER AND PASSWORD IS INCORRECT

Sold by **djamba15** - 311 sold since Jun 28, 2016 **Vendor Level 1** **Trust Level 4**

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 10.00

Qty: **Buy Now** **Queue**

0.0112 BTC / 0.8210 XMR

[Description](#) [Bids](#) [Feedback](#) [Refund Policy](#)

Product Description

I will send the USER and PASSWORD if it stops working just pm me and Ill replace it!
 WILL REPLACE ONLY IF USER OR PASSWORD IS NOT WORKING
 I CAN NOT GUARANTEE THE THE ACCOUNT WILL HAVE A CC ON FILE OR PAYPAL OR IF IT HAS A BALANCE, WILL NOT REPLACE THE ACCOUNT UNLESS USER AND PASSWORD IS INCORRECT

Figure 6 shows an Alphabay sale of Uber accounts. Most consumers fail to realize how much information is stored in their everyday accounts. For instance, Uber accounts include name, credit card information, geolocation data, etc. An adversary could target users based on their activities. For example, a nation-state APT might be interested in the travel logs of critical infrastructure personnel.

Americans receive little notice, knowledge, or choice, in how and whether their information is collected in mass dragnet surveillance by search engines, retailers, their healthcare network, or literally any organization present throughout their lives. Data brokers aggregate this information into individual, community, and societal profiles that are used to deliver focused advertisements, specialized recruitment strategies, and other personalized content. Due in part to the success of this vector and due to the widespread access to data sets concerning most consumers' information (as obtained from the plethora of Healthcare, Government, and other critical infrastructure breaches), information warfare attacks that leverage demographic and psychographic algorithmic insights, are developing to be the new normal in adversarial campaigns. Americans are poised to be manipulated and repeatedly victimized by adversaries who possess complex, granular-detailed personalized dossiers, knowledge of ingrained niche-community trends, and the ability to identify and influence triggers in segments of the U.S. population. This threat vector is possible because organizations, such as data brokers, failed to recognize their role as data stewards, and because data protectors, failed to secure data

according to its value to multiple stakeholders (including the data subjects themselves). Consequently, Americans are digitally pummeled in every breach, on every Deep Web market, and by every cyber-adversary.

The Product is “You”

Think about what value you would attribute to your demographic and psychographic information. For how much would you sell your name, birthday, online browsing history, etc.? Free online services collect users’ personally identifiable information (PII) (via cookies, web forms, and other vectors) and monetize it via targeted advertisements and via the collection and sale of data to third-party data brokers and data custodians (research entities, etc.). Data Brokers are willing to sell consumer demographic and psychographic information to advertisers and other third-parties for mere pennies per user profile; yet, few, if any, users would be willing to share that same information for the same price [2]. Financial Times and other sources offer digital calculators that predict exactly how much an online advertiser would pay for an individual’s data, as a mechanism of informing consumers of their stark monetary value [3]. One study that relied on refined Experience Sampling, probed users’ value of their own PII in comparison of the value attributed to offered services and found that typical users in 2013 valued their online browsing history at ~\$7 and valued their demographic information at ~\$36. Monitoring of user activity indicates that data generated from online financial activities and social media data were valued higher than search data or shopping profiles. Users in the study were indirectly monitored (i.e. the Observer Effect was limited). In their willingness to provide data to private entities, users did not distinguish between the quantity of PII exchanged (one field versus ten fields); instead exchange decisions depended on the type of PII (demographics, photos, etc.) requested. Users preferred to exchange PII for money, goods, and improvements in services followed by getting more free services and targeted advertisements [4].

Consumers rarely attempt to discover what information organizations are collecting about them via their daily activities and online interactions. Most will never read the tedious privacy policies meant to legally provide data subjects with this information. In fact, the “Terms and Conditions” and “Privacy Policies” are intentionally written to deter informed user decision making. The average user visits ~1500 different sites per year. The privacy policy on each site is approximately 2500 words (based on an average of the privacy policies of the top 75 websites). If, on all the sites that a user regularly visits, they read 250 words per minute, then the cost of visiting that site and becoming a marginally informed user is 10 minutes. Therefore, the average user would have to spend 25 days per year (or 76 days if their job was reading privacy policies only during workhours) just to be marginally informed (as opposed to well-versed) about how their data is collected and used. This nationally equates to 53.8 billion hours annually spent reading privacy policies in order to have even a marginally informed populace. The annual cost of making informed decisions (estimated at 25% of average hourly salary during leisure and at


twice wages during work) would be between \$2533 - \$5,038 per year (or \$781 billion nationally) [2]. For comparison, total online sales amounted to \$335 billion in 2015 [5]. Similarly, software and account settings that enable users to restrict the types, amount, and use of collected data, are often intentionally complicated, difficult to find or use, or are distributed and buried deep in recursive menus [6]. Standardized mechanisms of informing consumers of the disclosure of their demographic or psychographic information are necessary but are either absent or are insufficiently implemented in nearly every daily interaction between the average consumer and the organizations that collect, use, monetize, and manipulate their data [7]. When consumers are provided with privacy information as they make online decisions, they default to more privacy protective goods and services. For instance, if consumers were provided with the same product from similar online vendors, and the data collection information were easily communicated, then most users would intentionally choose to purchase the product or service of the more privacy protective organization, even if they had to pay a premium on the product [6]. As a result, organizations whose business models rely on the monetization of data intentionally prevent users from making informed decisions regarding their PII, EHRs, and other demographic and psychographic information. Hospitals, banks, search engines, and others now require users to “voluntarily” share their information in exchange for use of the network or service. Often, if the user does not share, then they cannot use the product or service. Because users are not informed as to what data are collected, which third-party organizations will acquire that data, or how that data will be used, the preponderance of consumers agree without even recognizing the interaction as a decision.

Americans Are Targeted More Successfully because America Lags Behind Global Privacy Initiatives

There is a dearth of data privacy protection regulation in the United States as compared to the rest of the world. Many countries, including those in the European Union, incorporate the Fair Information Practices (FIPs) into regulatory standards and laws. The FIPs are guidelines for data collection, use, and handling, focused around principles of: openness and operational transparency, individual access, data subject participation, data use, disclosure limitations, responsible information management, and accountability. In the United States, organizational adherence to the FIPs principles is predominantly voluntary and sporadic [8]. The most popular implementation, known as “Notice and Choice” is often an empty gesture because organizations hide the information concerning data collection, monetization, and utilization, within intentionally nebulous “Terms and Conditions” and “Privacy Policies” documents that consumers will never read and that act as more of a contract against consumer litigation than as a notice or offering of a choice. In 2011, the Obama White House issued a version of the FIPs in a National Strategy of for Trusted Identities in Cyberspace (NSTIC) report. The guidelines, meant for the public and private sector, promote: transparency in the collection, use,

dissemination, and maintenance of PII; individual participation and consent in relevant data processes; articulation of the specific purpose and authority for which data are collected and used; a minimization of collected data to only what is necessary and relevant; a limitation that collected PII should only be shared or used for the reasons expressed in the notification communicated to the data subject; provisions that organizations should ensure the accuracy and relevance of data; security safeguards to protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure; and accountability and auditing principles that include providing proper use training to personnel and contractors who access PII and an audit process that demonstrates the proper use of the data in compliance with the aforementioned guidelines, and all applicable privacy principles, requirements, or regulations [8][9].

Figure 7: Compromised Data Brokers Pose a Significant Risk to Americans



★WORLD FAMOUS™★ TEN 10 USA PROFILE Fullz Bank Details
Acc Routing SSN DL+★

WARNING THESE ARE NOT CC, THESE ARE USA DATA PROFILES * As some of the regulars will know I sold these on EVO for quite some time with excellent results report from customers This listing is for TEN 10 USA Full This listing works out at \$1 per record Other vendors are currently reselling OUR data at \$10 per record! We can supply ANY amount of info required Please check my store for our ...

Sold by **ThinkingForward** - 539 sold since Mar 21, 2015 **Vendor Level 1** **Trust Level 9**

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

10 USA NON CC FULLS (RANDOM) - 1 days - USD +0.00 / item

Purchase price: USD 10.00

Qty: **Buy Now** **Queue**

0.0112 BTC / 0.8210 XMR

[Description](#)
[Bids](#)
[Feedback](#)
[Refund Policy](#)

Product Description

WARNING THESE ARE NOT CC, THESE ARE USA DATA PROFILES *

As some of the regulars will know I sold these on EVO for quite some time with excellent results report from customers

This listing is for TEN 10 USA Full This listing works out at \$1 per record Other vendors are currently reselling OUR data at \$10 per record!

We can supply ANY amount of info required Please check my store for our different amounts With our 100 info listing the price drops to only \$0 50 per record and even more for larger amounts :)

firstname	phone_cell
middlename	contact_time
lastname	email
ssn	ip_addr
date of birth	pay_frequency
mmn	net_income
dl_number	employment_status
dl_state	employer_name
gender	job_title
military_active	phone_work
amount_requested	phone_work2
residence_type	bank_name
residence_length	account_type
address1	direct_deposit
address2	reference1_firstname
city	reference1_lastname
state	reference1_relationship
zip	phone_reference1
phone_home	reference2_firstname
phone_cell	reference2_lastname
contact_time	reference2_relationship
email	phone_reference2
ip_addr	routing_no
pay_frequency	account_no
net_income	lead_status
employment_status	lead_status_leadlab
employer_name	
job_title	
phone_work	
phone_work2	
bank_name	
account_type	
direct_deposit	

Figure 7 shows the sale of consumer profiles, “fullz”, that were extracted from an inadequately protected Data Broker database and it shows some of the fields that might be stolen in such an incident. The sample information shown can be used in precision targeted campaigns against high-profile individuals or critical infrastructure personnel.

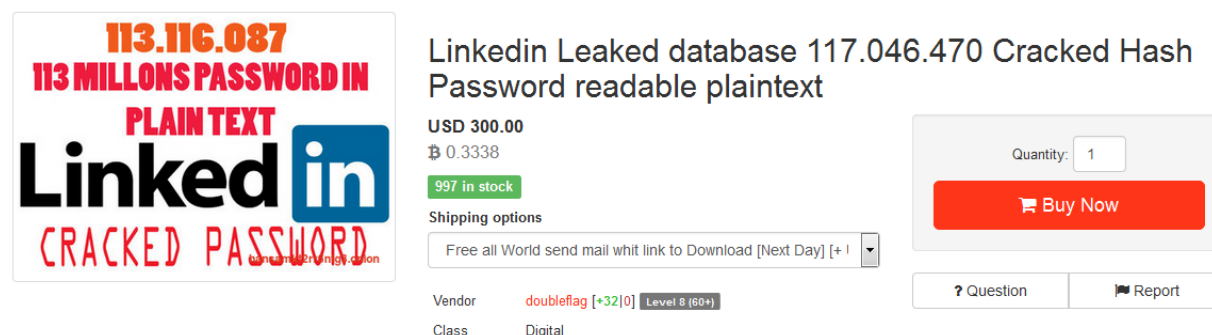
By contrast, the European Union's 1995 Data Protection Directive allowed data subjects to request the rectification, erasure or blocking of the processing of inaccurate, incomplete, and outdated data, and it required the data custodians to notify associated third parties to whom the data had been disclosed, of necessary commensurate operations on the same data [10]. As of May 2014, the European Union has granted citizens the "Right to be Forgotten" as a modernization of the 1995 Data Protection Directive. The modernization also included provisions such as data portability, data breach notifications, etc. The "Right to be Forgotten" provides that under certain conditions, individuals have the right to ask search engines to remove information that is too personal or that is inaccurate, inadequate, irrelevant or excessive, for the process of data processing. It is worth noting that the ruling is not absolute; it only necessitates that organizations (search engines, etc.) operating in the European Union (regardless of the physical location of their server) provide a mechanism for individuals to request the deduction of personal data in the aforementioned categories, pending a case-by-case assessment by the hosting entity. The assessment considers the type of information, its sensitivity and effect on the individual's private life, the requestor's public role, and any interest the public might have in access to the information. The ruling does not allow individuals to pick and choose what data are collected or utilized, it does not make prominent people less prominent, and it does not reduce the notoriety of criminals. Additionally, hosting companies are required to delete data if a court or regulatory body rules in favor of an individual. The ruling attempts to balance individuals' rights of data protection with the economic interests of search engines and data hosts. Further, the right to be forgotten cannot be used to subvert other fundamental rights such as freedom of expression and the media. The burden of proof that data cannot be deleted because it is still relevant or is needed is shifted from the consumer to the organization. Organizations who fail to comply with the "Right to be Forgotten" and other EU modernization provisions may be subject to fines of up to 2% of annual worldwide turnover [10].

Who Are Data Brokers?

Data brokers are organizations who collect, aggregate, and monetize consumer data from a wide range of information streams. Data are collected from: government and public records, court filings, property and tax assessor records, liens, mortgages, driver's license records, voter registration records, telephone directories, professional licenses, birth/ marriage/ divorce records, recreational licenses, Census demographic information, warranty cards, sweepstakes/ contest/ survey entries, social media profiles and preferences (Facebook, LinkedIn, etc.), web-browsing activity, data collected by advertising networks, catalog/ magazine information, website registration information, email information, healthcare network information (forms, questionnaires, etc.), purchasing history information, and from a wide range of other sources. In general, if consumer information is generated, then a company exists that is interested in the

collection and analysis of that data. Information is aggregated into niche categories and is then used to generate detailed individual and societal profiles, which are subsequently sold or shared with additional external third-party organizations [11] [12].

Figure 8: Compromised Professional Social Media Networks can be used in Psychographic Attacks

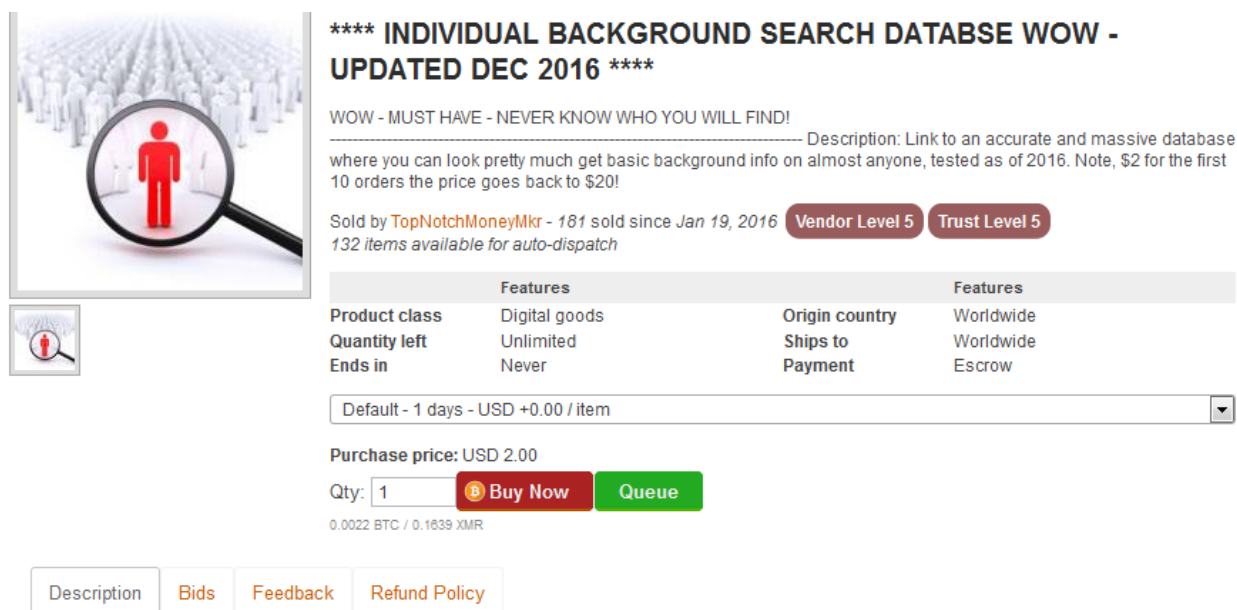


Social networks such as LinkedIn can be used to steal additional information, to build complex profiles, or to spread psychographic lures to networks and into niche-communities. Adversaries can spoof LinkedIn, mimic a contact, or leverage an interest, in precision focused lures sent to specific critical infrastructure professionals.

The FTC categorizes data brokers into three varieties based on the product that they sell.

1. **Marketing Products Data Brokers** offer products, services, and platforms that tailor marketing messages to consumers, on behalf of client organizations. This includes direct marketing (mail, telemarketing, and email), online marketing (Internet, mobile device, and Satellite television), and marketing analytics that attempt to predict consumer behavior. Marketing products tend to rely on information provided by affiliates, and the data may not always be current or matched to the correct individual [11].
2. **Risk Mitigation Data Brokers** are sub-categorized based on whether they sell identity verification or fraud detection services. Identity verification products are used by banks and other clients to confirm the identity of an individual; meanwhile, fraud detection products are used by clients, such as government agencies, to verify the reliability or integrity of user submitted information. Risk Mitigation data sources engage integrity and verification processes to ensure that collected data are accurate and reliable [11].

Figure 9: Adversaries have Already Compromised Entire American Background Check Databases



****** INDIVIDUAL BACKGROUND SEARCH DATABASE WOW - UPDATED DEC 2016 ******

WOW - MUST HAVE - NEVER KNOW WHO YOU WILL FIND!

Description: Link to an accurate and massive database where you can look pretty much get basic background info on almost anyone, tested as of 2016. Note, \$2 for the first 10 orders the price goes back to \$20!

Sold by **TopNotchMoneyMkr** - 181 sold since Jan 19, 2016 132 items available for auto-dispatch

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty: **Buy Now** **Queue**

0.0022 BTC / 0.1639 XMR

Description Bids Feedback Refund Policy

Product Description

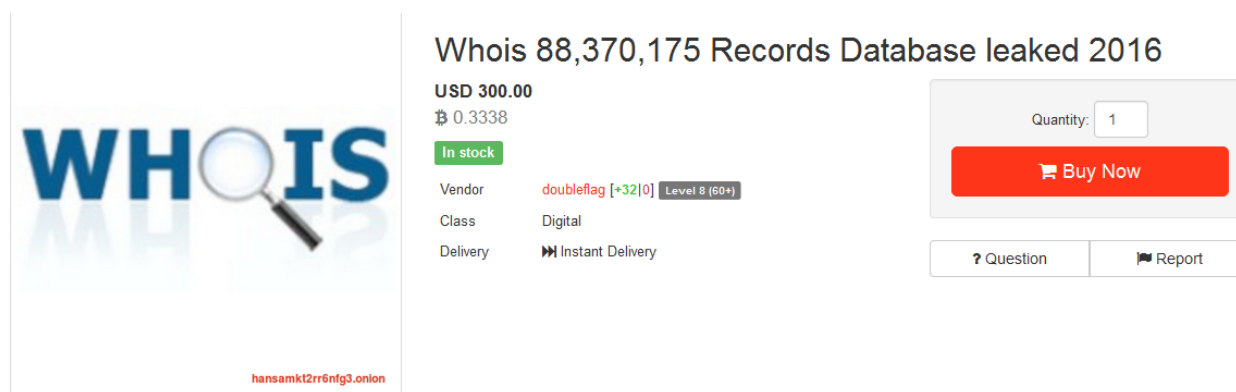
WOW - MUST HAVE - NEVER KNOW WHO YOU WILL FIND!

Description: Link to an accurate and massive database where you can look pretty much get basic background info on almost anyone, tested as of 2016. Note, \$2 for the first 10 orders the price goes back to \$20!

Figure 9 is a screenshot of a the Alphabay sale of background checks from a compromised Data Broker database. A background check provides enough information to exploit an individual (such as a critical infrastructure employee, say a ICS/SCADA admin); meanwhile, a database of background checks provides the information necessary to exploit the general population or to target critical infrastructure.

3. People Search Data Brokers provide individual consumers, law enforcement, private investigators, the media, and others, with select fields of personal information about other individuals [11]. Over 300 online people service products exist, and the services are often used for nefarious purposes such as stalking. People Search Data Brokers rarely assess their data for accuracy or take steps to ensure that the correct data are matched to the correct individual [11].

Figure 10: Cyber Threat Actors have also Breached People Search Engines



Whois 88,370,175 Records Database leaked 2016

USD 300.00
₿ 0.3338

In stock

Vendor: **doubleflag** [+32][0] Level 8 (60+)

Class: Digital

Delivery: **Instant Delivery**

Quantity: 1

Buy Now

? Question Report

hansamkt2rr6nfg3.onion

Listing Details

88M+ Database file is stored in a 80GB+ split files to better download records 88,370,176 of all world
(THIS DATABASE NEVER BE A PART OF ALL LEAKED DATABASE PACKAGE)

fields records:

domainName, registrarName, contactEmail, whoisServer, nameServers, createdAt, updatedAt, expiresDate, standardRegCreatedAt, standardRegUpdatedAt, standardRegExpiresDate, status, registrant_email, registrant_name, registrant_organization, registrant_street1, 16registrant_street2, registrant_street3, registrant_street4, registrant_city, registrant_state, registrant_postalCode, registrant_country, registrant_fax, registrant_faxExt, registrant_telephone, registrant_telephoneExt, administrativeContact_email, administrativeContact_name, 29administrativeContact_organization, administrativeContact_street1, administrativeContact_street2, administrativeContact_street3, administrativeContact_street4, administrativeContact_city, administrativeContact_state, administrativeContact_postalCode, 37administrativeContact_country, administrativeContact_fax, administrativeContact_faxExt, administrativeContact_telephone, administrativeContact_telephoneExt, billingContact_email, billingContact_name, billingContact_organization, billingContact_street1, 46billingContact_street2, billingContact_street3, billingContact_street4, billingContact_city, billingContact_state, billingContact_postalCode, billingContact_country, billingContact_fax, billingContact_faxExt, billingContact_telephone, billingContact_telephoneExt, 57technicalContact_email, technicalContact_name, technicalContact_organization, technicalContact_street1, technicalContact_street2, technicalContact_street3, technicalContact_street4, technicalContact_city, technicalContact_state, technicalContact_postalCode, 67technicalContact_country, technicalContact_fax, technicalContact_faxExt, technicalContact_telephone, technicalContact_telephoneExt, zoneContact_email, zoneContact_name, zoneContact_organization, zoneContact_street1, zoneContact_street2, zoneContact_street3, 78zoneContact_street4, zoneContact_city, zoneContact_state, zoneContact_postalCode, zoneContact_country, zoneContact_fax, zoneContact_faxExt, zoneContact_telephone, zoneContact_telephoneExt, registrarIANAID

Whois provides domain name and IP registrations. Figure 7 depicts the Deep Web sale of over 88 million Whois records. Big Data analytics of these records could be used for internet mapping, to find relationships between sites, or to plan an exploit campaign based on lateral breaches on shared infrastructure.

According to the FTC, data brokers are only compelled to maintain the privacy of consumer data if those data are used for credit, employment, insurance, housing, or similar purposes. The Fair Credit Reporting Act (FCRA) only applies to data brokers, as consumer reporting agencies (CRAs), if the data are used in decision making processes by the issuers of credit or insurance, or by employers, landlords, and others in making eligibility decisions affecting consumers. Further, consumers do not have a right to know what information data brokers have compiled about them for marketing purposes. Consumers lack any right to correct inaccuracies in the data or in assumptions made by data brokers [13]. The Data Security and Breach Notification Act would have been the first U.S. federal law requiring data brokers to inform consumers when hackers have stolen their data; however, it has been proposed and killed in Congress every year since its conception in 2009. The Data Broker Accountability and Transparency Act of 2015 suffered a similar fate [14].

It is not difficult to obtain sensitive data from a data broker. As discussed below, data brokers are frequently breached or knowingly sell data to malicious organizations. For example, a 24-year old cybercriminal, Hieu Minh Ngo, spoofed an American company title and gained access to the demographic and psychographic data of 200 million Americans maintained by Experian, one of the three main credit bureaus. There is practically nothing in terms of morals, oversight, or other controls preventing a data broker from selling data to a nation-state operated organization or directly to a nation-state sponsored Advanced persistent threat, who will then use the data in hybrid information warfare campaigns that target America's critical infrastructure sectors or that further victimize average consumers, whose data was collected without sufficient notice and without their informed choice.

Problem 1: Data Brokers Operate in the Shadows

Demographic categorization is the process of grouping population subsets according to externally measurable variables, such as gender, age, income, marital status, etc. [15]. Collected demographic information might include names, addresses, telephone numbers, email addresses, age, gender, family statuses, Social Security numbers, religion, real estate data, political affiliation, estimated income level, education level, occupation, and other information [11]. The information exfiltrated in most cybersecurity breaches is demographic data. However, psychographic data may be exposed in some incidents, such as in the OPM breach, where granular 127 page SF-86 forms were exfiltrated by the Deep Panda APT. The stolen information will be weaponized to impact American critical infrastructures for decades to come.

Psychographic targeting is the process of segmenting a population according to variables pertaining to interests, attitudes, and opinions (IAO variables) and then tailor focusing a campaign to target select demographic subsections, in order to magnify the appeal of the campaign and the likelihood that the select users will positively respond. IAO variables might include purchasing habits, hobbies, browsing time, medical condition information, preferred payment methods, and life triggers (having children, moving, buying a home, etc.) [16]. Marketing and other campaigns rely on demographics to define "who" buyers are and they rely on psychographics to explain "why" those users buy [15].

Demographic information is often publicly available (Census, social media, etc.) while psychographic information is collected by first and third-party networks. Psychographic information is the defining product of the data broker industry. The collection of psychographic variable data does not require direct interaction with the user; in fact, it often depends on the inaction of average consumers [17]. Every piece of information entered into a hospital form, every shred of data provided when applying for a discount card, every completed social media profile field, every web search, etc. has the potential to be collected and sold to interested third-parties. The primary control afforded to consumers comes in the form of opt-out options, which are all-too-often hidden within recursive menus or in the exhaustive "Terms and

Conditions” or “Privacy Policy”. Default settings are typically configured to collect as much user information as possible. Though notice and choice of data collection and potential sale, is offered to the consumer, convenience and incentives (use of a network, discounts, etc.) are often heavily leveraged against the collection target because modern business models depend upon the sale of user data as the principal revenue stream. This exchange as a process is neither inherently beneficial nor nefarious. To a degree, any rational consumer understands that when they provide data to an information steward, that it may be capitalized upon or utilized in background processes. Products and services are not free. There are always hidden costs associated with free social media, free search engines, free operating systems, free programs, etc. In order to use the offerings of Facebook, Google, Apple, Microsoft, and others, the rational user exchanges their data for the incentive or utility offered. However, consumers often fail to comprehend exactly how their data are monetized, who purchases the data, and how those data are further used and resold. For instance, with just consumer provided information such as likes, preferences, and an email address, an organization can tailor advertisements, send focused newsletters and emails, and “suggest” social media content [18].

Data brokers and data analytic firms purchase or manage first-party information from sources such as social media, “free” services, etc. and then they categorize and resell the anonymized or pseudo-anonymized data to marketing firms and other buyers. Brokers are differentiated by their information streams, their analysis algorithms, and their data categorizations. For instance, some firms assess individuals along dimensions such as: Openness, Conscientiousness, Extraversion, Agreeableness and Neuroticism. The dimensions are then further subcategorized and then predictive models are calibrated and run against large datasets in order to anticipate and ascertain normalized psychological models that are characteristic of subsets of consumers. The amount of information compiled from various information streams rapidly compounds. For example, one firm, Cambridge Analytica, publicly claim to have over 5,000 data points on every American voter [17]. Tens of thousands of additional data points might be measured by other firms. The goal of the collection of demographic and psychographic information is to predict and model the behavior of every individual using as many variables as possible in order to sell the ability to reliably influence or manipulate the behavior of a population as a whole. Brokers offer the models, analytic tools, and data as products and services to additional firms. Data brokers’ products often includes graphical interface and data visualization tools that enable these firms to easily determine and predict information about millions of individuals and hundreds of population subsets by pressing only a few buttons [17].

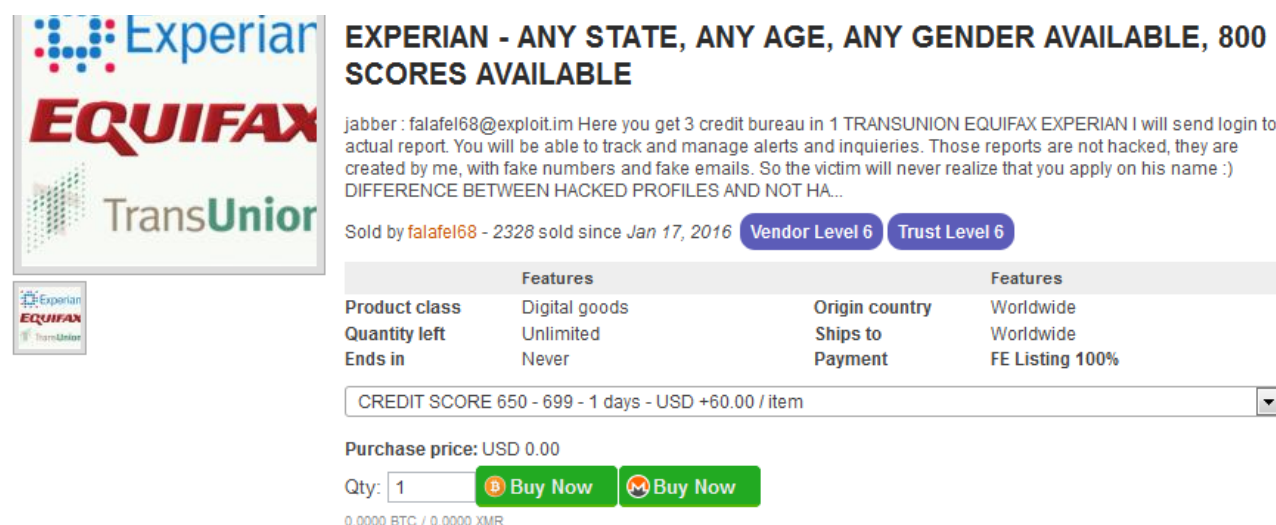
Data brokers have a history of utilizing data in ways that are contrary or harmful to consumers’ interests and a history of lackadaisical cyber-hygiene and cyber-security. In her August 2013 keynote speech at the Technology Policy Institute’s Aspen Forum, FTC Chairwoman Edith Ramirez said ““Firms of all sorts are using consumer data in ways that may not just be contrary

to consumers' expectation, but could also be harmful to their interests. This problem is perhaps seen most acutely with data brokers — companies that collect and aggregate consumer information from a wide array of sources to create detailed profiles of individuals. Their success depends on having more and better data than their rivals. The concern is that their mega-databases may contain highly sensitive information. The risk of improper disclosure of sensitive information is heightened because consumers know nothing about these companies and their practices are invisible to consumers" [19]. Data brokers, who are subject to minimal oversight, have a history of gross negligence and abuse, in their positions as data stewards. As a result, members of the general population, who often are not aware that their data profile is collected, who it is sold to, or how it is used, are victimized.

Where Do Brokers Acquire Data?

Data Brokers aggregate information from as many data streams as possible. An FTC report that followed just nine data brokers found that brokers obtained: the purchase history of 190 million individual consumers from 2,600 retailers; mobile carrier information; automotive dealer sale, service, warranty, and aftermarket repair information; consumer self-reported information from online surveys, warranty registrations, and contests. One broker allegedly compiled and maintained 1,000 categories of self-reported information from 240 million Americans [16]. Data brokers purchase information from retailers (purchase history), magazines (subscription information), the Department of Motor Vehicles (PII), Experian and other credit reporting agencies (lists of data as granular as parents expecting newborns, etc.), real estate records, voting data, etc. [20]. According to Federal Trade Commission (FTC) Chairwoman Edith Ramirez, "The extent of consumer profiling today means that data brokers often know as much – or even more – about us than our family and friends, including our online and in-store purchases, our political and religious affiliations, our income and socioeconomic status, and more" [16]. Companies that buy or sell data tend to keep exchanges as quiet as possible in order to avoid the attention of the general public [1]. The following sections detail some of the subsectors that provide massive amounts of information to Data Brokers that can be used in multi-vector information warfare cyber-campaigns paired with psychographic and demographic Big Data analytics.

Figure 11: America's Credit Unions Fail to Secure Data by Verifying Data Brokers' Identities and Protecting Databases



EXPERIAN - ANY STATE, ANY AGE, ANY GENDER AVAILABLE, 800 SCORES AVAILABLE

jabber : falafel68@exploit.im Here you get 3 credit bureau in 1 TRANSUNION EQUIFAX EXPERIAN I will send login to actual report. You will be able to track and manage alerts and inquiries. Those reports are not hacked, they are created by me, with fake numbers and fake emails. So the victim will never realize that you apply on his name :) DIFFERENCE BETWEEN HACKED PROFILES AND NOT HA...

Sold by falafel68 - 2328 sold since Jan 17, 2016 **Vendor Level 6** **Trust Level 6**

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

CREDIT SCORE 650 - 699 - 1 days - USD +60.00 / item

Purchase price: USD 0.00

Qty: **Buy Now** **Buy Now**

0.0000 BTC / 0.0000 XMR

The listing depicted in Figure 11 offers credit reports based on desired victim credit scores. This means that the adversary has the ability to gain access to the three credit unions or to a third-party that can request that information. The cybercriminal is selling the information for identity theft, but they could just as easily sell it to a nation-state threat actor. These reports provide an adversary with all the information needed to exploit an individual or to psychographically profile a population subset according to IAO variables.

The Cost of Socialization

Users voluntarily seek out social networks and they convince their friends and family to join. Every user provides profile information (demographic and psychographic) when joining. Some of that information is publicly displayed (and therefore available to cyber attackers) while other data are stored on the company server [21]. Facebook offers services to over 1.7 billion users, Google+ has over 540 million users, LinkedIn serves over 277 million users, and Twitter provides over 248 million users with a platform [23] [21]. Each and every user on every single platform is constantly and often, unknowingly, providing the platform host and their affiliated third-parties, with a relentless stream of valuable demographic and psychographic information. Have you ever noticed how the advertisements on social network sites mirror recent searches or interests? Psychographic data are used to serve particular ads to specific consumers based on likes, profile, web searches, etc. Social media platforms also monitor changes in user demographic and psychographic information. Have you recently lost your job? Have you visited or moved to a new city? Has your relationship status recently changed? Facebook and other social media platforms use psychographic analysis to know all of that information and to serve tailored advertisements, even if the user does not specifically provide the data [21]. Because minimal regulation or oversight has curbed these collection and analyses, cyber adversaries now have the capability to digitally scrape social media sites for information, to purchase data,

or to breach servers and exfiltrate data, algorithms, and predictions, to weaponize against consumers in targeted community campaigns and in personalized attacks.

Figure 12: Social Media Accounts Can Facilitate the Propagation of Psychographic Lures



The screenshot shows a listing for 'Facebook Account Hacker V 2.4' on a Deep Web market. The listing includes a title, a description, a table of features, and purchase options.

Product Title: AMAZON FACEBOOK TWITTER , VINE, SKYPE, ORGIN, INSTAGRAM, AIM ACCOUNT HACKER : 7 LEFT: + GIFTS

Description: EVERY WANTED TO HACK INTO YOUR GIRLFRIENDS FACEBOOK OR AN AMAZON ACCOUNT LET THIS PROGRAM DO IT FOR YOU IT IS MADE BY PROFESSIONALS FOR PROFESSIONALS VIDEO HERE <https://youtu.be/8iCSwAUYYOs> This software can get into any of the following accounts AIM Facebook AMAZON HULU INSTAGRAM netflix Orgin Skype Spotify Steam Twitter Vine Wether you want to gain access to social me...

Sold by: ineedaspo - 131 sold since Jun 30, 2016 **Vendor Level 3** **Trust Level 5**
285 items available for auto-dispatch

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 5.99

Qty: 1 **Buy Now** **Queue**

0.0087 BTC / 0.4908 XMR

Social media accounts, such as those for sale on the Deep Web market Alphabay, depicted in Figure 12, can be used to build profiles of individuals, to laterally target others in their networks, or to spread disinformation, fake news, propaganda, malvertising, lures, etc. across those networks. Exposure to these lures desensitizes the population and eventually, users will click on them despite cybersecurity and cyber-hygiene best practices.

Users believe that they are exchanging little or no information in exchange for a temporary distraction mechanism or a socialization platform; in reality, the social network monetization model is only slightly different than that of its media company predecessors. The “service” company is renting users’ attention to advertisers. The main difference is that social networks also collect and sell information to third-party affiliates for demographic and psychographic analysis. These functions are not side revenue streams; they are the entire purpose of the platforms. These revenue streams are what allow the platforms to be “free” to users and the model also facilitates dynamism and growth. Consider that Facebook’s 10-k filing with the U.S. Securities and Exchange Commission (SEC) includes the 2015 average revenue per user (APRU) at \$5.32 [23]. Similarly, Twitter’s SEC filing features the forward-looking statements such as "Our ability to attract advertisers to our platform and increase the amount that advertisers spend with us" and "Our ability to improve user monetization, including advertising revenue per timeline view" [23]. Facebook reported a 57% revenue increase in the first quarter of 2016; thereby, increasing its worth to \$5.2 billion. Revenue from mobile adverts on phones and other mobile devices accounted for approximately 80% of that revenue. Advertisers pay premiums to

advertise to mobile devices because the ads reach a wider subset of the population. Malicious threat actors may leverage demographic and psychographic data analysis to target BYOD devices through focused malvertising, fake news, and other vectors, in order to infect the less secure, higher trafficked, and more popular mobile devices. Infected mobile devices can then be used in cyberespionage campaigns against critical infrastructure personnel or to laterally infect critical infrastructure networks with malware.

Mobile Data Travels Further than Mobile Devices:

Figure 13: Apple Phishing Page Listing on Hansa Market



Apple Scam Phishing Page Get your own Fullz

Apple Website Payment phishing page get your own fullz and enjoy

Sold by **shonajaan** - 178 sold since May 14, 2015 **Vendor Level 5** **Trust Level 6**

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 3.30

Qty: **Buy Now** **Queue**

0.0037 BTC / 0.2703 XMR

Description **Bids** **Feedback** **Refund Policy**

Product Description



Apple Website Payment phishing page get your own fullz and enjoy

Apple and other mobile carriers automatically backup users' content. Adversaries can access this content by tricking users into entering their information into spoofed login pages. This information can be used to exploit the individual or it can be collected in bulk and sold to a more sophisticated adversary for psychographic analysis.

Cellular networks keep detailed, up-to-the-minute records of device locations through cell tower triangulation, they keep logs of incoming and outgoing communications, and most offer default digital backup services that store all of a consumer's data on a remote server (i.e. the cloud). Governments and law enforcement have long held the ability to compel carriers to provide customer tracking information; however, rather than provide that information at the request of an ongoing investigation, some companies are reportedly marketing tailored technology and databases to law enforcement and intelligence communities. These companies either purchase user information from carriers or collect it themselves via mobile applications, or software embedded in the devices. At some level, most rational adults who use mobile

devices know that they can be tracked; however, few users realize that their geolocation data are further sold off or is collected by third-parties so that it can be used in campaigns that target the user [22]. For instance, this data might be sold to local marketers or advertisers to create tailored direct-mail advertisements to send to consumers' homes based on their local shopping habits and travel patterns.

Figure 14: Attackers can Send Android Malware to Stolen Demographic Profiles

DROIDJACK - ANDROID RAT -

Hi, you can buy this Android RAT. It has a lot of function and you can take control of your victim's android phone! VERY POWERFUL Developer ask for 210\$ but I'm Santa Claus and give it to you for just \$1.10 :D ★ABOUT US★
Pringleships is a level 5 shop with more than 2300 successful transactions on AlphaBay Market. You can message our customer service for any question you may have.

Sold by **pringleships** - 512 sold since May 27, 2015 **Vendor Level 5** **Trust Level 5**

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Autofulfill - 1 days - USD +1.09 / item

Purchase price: USD 0.01

Qty: **Buy Now** **Queue**

0.0000 BTC / 0.0008 XMR

[Description](#)
[Bids](#)
[Feedback](#)
[Refund Policy](#)

Product Description

Hi, you can buy this Android RAT. It has a lot of function and you can take control of your victim's android phone! VERY POWERFUL Developer ask for 210\$ but I'm Santa Claus and give it to you for just \$1.10 :D

★ABOUT US★

Pringleships is a level 5 shop with more than 2300 successful transactions on AlphaBay Market. You can message our customer service for any question you may have.

Adversaries can leverage marketing, retail, and other breaches to target consumers with SMS and email lures that install Remote Access Trojans on their systems. These malware provide the attacker with complete control over the system and facilitate further information collection and cascading incidents (botnets that spread SMS malware to contact lists, etc.).

Even if a consumer is aware that geolocation data are collected and paired with their demographic or psychographic data, that same user may not be aware that the data are sold to third-parties. Further, many of the organizations that collect data and market geolocation services operate or originate within foreign nations [22]. The facts combine into a series of dismal potentials for Americans whose data are collected, stored, and monetized, by domestic and foreign data brokers. A cybercriminal could breach Telecommunications servers and exfiltrate consumer backups, stored credentials, communications, etc. Nation state threat actors could simply obtain the data from domestic telecommunication organizations or data

brokers. The contents of a users' mobile communications, mobile browsing history, associated accounts, tracking information, etc. can be used to craft personalized social engineering lures. For example, an adversary could obtain the aforementioned data and then identify users who work at a specific critical infrastructure facility by either following their mobile geolocation data (i.e. which users visited this location) or by cross-referencing the stolen data with social media networks (Facebook, LinkedIn, etc.). Next, the threat actor could tailor a personalized lure (SMS, VOIP, social media message, email, etc.) to the user based on psychographic analysis of the user. If the target receives a lure tailored to their interests, on their personal device, then they may not even consider cybersecurity or cyber-hygiene commensurate with their profession. The lure could deliver malware onto the personal device, and then use it to laterally move onto the network.

Healthcare Data Exchanges Contribute to The Industry's Vulnerability

United States Hospitals, Health Insurers, and other healthcare organizations are entrusted with patients' healthcare information in order to facilitate the physical and mental well-being of their patients. These organizations are trusted to protect the very information that defines a person. Most do not question healthcare organizations when asked to provide information on form after form, because they presume that the data will be used to ensure that they receive the highest quality care. Little do they know, healthcare organizations are betraying their duty, betraying their patients, and betraying the very Hippocratic Oath that once defined the sector. For the most part, the electronic health record (EHR) system is so opaque that doctors, nurses, and patients are unaware that the information recorded in an EHR may be sold to external third-parties. Federal laws and regulations, such as HIPAA, the HIPAA Privacy Rule, etc. establish stringent standards regarding the use and dissemination of personal health information (PHI). Nevertheless, states such as Arizona, Texas, New York, New Jersey, and Washington are selling "anonymized" healthcare data via a "state exemption" from federal regulations that allows states to sell large volumes of "hospital discharge data" for profit to data brokers and consumer reporting agencies. This anonymized data can be used for psychographic data analysis or it can be de-anonymized using public information, for targeted attacks against high-profile individuals. In 2011, twelve of the most populous states generated \$1.91 million from 1,698 exchanges. Public and private companies, many of which claim to be "credit reporting agencies", are the most frequent multi-state health profile buyers [24]. The provisions allowing for the aggregation and exchange of PHI was intended to facilitate insights and innovations in the research community by generating larger, more focused data sets that were more characteristic of the population as a whole [1]. While research does advance from this practice, for the most part, data subjects see no fiscal dividends and limited benefits from the sales of their PHI that occur without any meaningful attempt at securing informed notice or choice. As a result, patients have no notice or control over the sale of data that defines their identity and existence. Organizations affiliated with an enemy nation-state, that are infiltrated by an insider

threat, or that have been breached, may pass granular healthcare data onto cyber-threat actors.

Some hospitals and healthcare networks claim to buy and sell patient data in order to identify “high-risk” patients, such as smokers, and to curtail negative health habits. Hospitals who buy data can cross reference credit or debit history, online browsing data, and other information with electronic health records, to psychographically profile individuals. The practice is of highly-questionable moral and ethical grounds, but it may be worthwhile to for-profit hospitals that wish to preclude accepting patients with pre-existing conditions, patients whose families might sue, patients unable to afford care, etc. In the best case scenario, this data are used to monitor broad and localized societal healthcare trends. The more data incorporated into the predictive algorithms, the more accurate the predictions [20]. The downside to this practice, other than the numerous nefarious business practices it could facilitate, is that healthcare organizations are already high value targets of cybercriminals, cyber-mercenaries, nation state APTs, and other cyber threat actors, that covet the expansive, often under-secured, treasure troves of information stored. Additional information purchased from external third-parties adds even more information to the trove and increases the appeal for an attacker to target a healthcare organization.

One example purchaser of this data is IMS Health, which has curated some of the most detailed prescription drug and medical health dossiers on over 260 million United States citizens. Globally, the organization may have assembled over half a billion patient dossiers. IMS Health generated \$2.6 billion in revenue in 2014. IMS won a 2011 Supreme Court case allowing it to gather and exchange medical patient data, on the grounds of corporate “free speech”, despite the contention of 36 states, the Department of Justice, and numerous medical and consumer advocacy groups. IMS automatically receives petabytes (one-million gigabytes) of data from the EHR information held by pharmacies, insurance companies, medical organizations, and state and federal health departments. An estimated three-fourths of all retail pharmacies in the United States send electronic records to IMS Health [1]. IMS Health and similar healthcare data brokers, circumvent medical privacy rules by designing their records to be pseudo-anonymous or anonymous. Some of these records only contain year of birth, gender, partial zip code and doctor's name. The company leverages Big Data psychographic and demographic analytics on the data and offers the resulting predictions, behavioral analyses, and trends to pharmaceutical companies, which use the data to design sales pitches to deliver to doctors and direct-mail and online-ads campaigns to target consumers. Massive stores of hyper-detailed information (even anonymous or pseudo-anonymous data) such as that curated in IMS Health, is a colossal target for cyber adversaries that can leverage the data in broad and precise campaigns against individuals and against critical infrastructure systems [24]. This data could be obtained in

sophisticated campaigns such as the Deep Panda breach of OPM; in fact, Deep Panda has a history of attacking healthcare organizations, such as Anthem, CareFirst, and others.

Adversaries can also breach the systems of data brokers that focus on niche professionals in targeted attacks on the healthcare sector and other critical infrastructure organizations. For instance, one example broker offers customers a hospital database of 2.1 million profiles relating to U.S. healthcare providers and decision makers at over 480,000 healthcare facilities. The database contains the names, emails, mailing addresses, and contact information of “the country’s most influential hospital executives” for the purpose of hiring and other decisions. The data also contains specific information such as hospital bed counts, site types, ownership information, etc. The service is telephone-verified and offers numerous licensing options, quarterly updates, and some data-processing services [25]. A cyber adversary could obviously purchase or compromise brokers such as this in order to precision target high-value healthcare professionals or to conduct Big Data psychographic predictive analysis on the United States healthcare sector as a whole.

Figure 15: Professional Recruitment Organizations’ Data Treasure Troves are Significant Cyber-Targets



The screenshot shows a product listing for a database of 122,957,027 records. The product is titled "B2B USA COMPANY 122.957.027 RECORDS DATABASE LEAKED 2016". The price is listed as USD 500.00 and ₪ 0.5563. It is marked as "In stock". The vendor is "doubleflag" with a rating of [+32|0] and a level of 8 (60+). The class is "Digital" and the delivery is "Instant Delivery". There is a "Buy Now" button and a "Report" button. Below the listing, there are links for "Details" and "Feedback".

B2B USA COMPANY 122.957.027 RECORDS DATABASE LEAKED 2016

USD 500.00
₪ 0.5563

In stock

Vendor: doubleflag [+32|0] Level 8 (60+)

Class: Digital

Delivery: Instant Delivery

Quantity: 1

Buy Now

? Question Report

Details Feedback

Listing Details

B2B USA COMPANY 122.957.027 RECORDS DATABASE LEAKED 2016
(THIS DATABASE NEVER BE A PART OF ALL LEAKED DATABASE PACKAGE)

Records come with Important Decision Maker Titles such as:

Associate Vice President of Marketing, Administrative Officer, Trustee, Grant Officer, Communications Manager, Administrative Assistants, Senior Training Specialist, Regional Sports Managing Director,

Marketing Director, Vice President, Regional Marketing Director, Director of Sports Marketing, Client Relationship Executive, Marketing Communications Manager, Senior Project Manager,...

Fields of database

email,sic_code,naics_code,company_name,contact_name,first_name,last_name,title,address,address2,city,state,zip,phone,fax,company_website,revenue,employees,industry,desc

Compromised niche-community and professional recruiting services databases provide adversaries with a powerful tool for customizing attacks against specific high-value personnel or against critical infrastructure sectors. For instance, lures can be focused to niche topics or can spoof trusted correspondence.

Problem 2: Fact: Data Brokers are Historically Negligent

Cyberattacks against data brokers are not a new trend. Below are but a handful of publicly disclosed data broker breaches. In most cases, the information was either used for identity theft, sold, or exploited in unknown ways. Data brokers fail to secure data according to its value, they fail to practice fundamental cyber-hygiene or moral business practices, and they ultimately fail to protect tens of thousands of data points on every American, from being obtained or exfiltrated by an adversary and subsequently exploited or leveraged in future attacks that repeatedly victimize data subjects, who had the bare minimum knowledge or consent over the collection, use, and monetization of their data. Further, sophisticated adversaries can leverage the demographic and psychographic data in multi-vector hybrid information warfare campaigns that target critical infrastructure or that undermine American Democracy.

ChoicePoint (2004, 2006)

ChoicePoint was a spinoff of Equifax's Insurance Services Group. In 2004, ChoicePoint, Inc. suffered a breach that compromised more than 163,000 consumers and that resulted in at least 800 cases of identity theft. Two years later, ChoicePoint suffered another breach (unauthorized access lasting over 30 days) that compromised 13,750 additional records [26]. ChoicePoint is a data broker and credentialing service that maintains over 19 billion data elements (name, SSN, date of birth, employment data, credit history, etc.) related to over 220 million Americans. An estimated 70% of ChoicePoint's revenue was generated from selling customer leads, background checks, and verification services to an estimated 100,000 clients ranging from marketing firms, to human resources departments, to government agencies, and to other entities, for insurance claim verifications and workplace background checks. In February 2008, ChoicePoint was purchased by Reed Elsevier and was rebranded as LexisNexis Risk Solutions [26].

Figure 16: Stolen Background Check Data Facilitates Cascading Breaches



How To Get a Background Check And Credit Report On Anyone 2016

USD 3.99
₿ 0.0046

In stock

Vendor: **Zloy3** [+2199|-34] [Level 10 (3000+)] ★ Trusted Vendor

Class: Digital

Delivery: 🚚 Instant Delivery

Quantity: 1

Buy Now

? Question Report

[Details](#) [Feedback](#)

Listing Details

Having this information can be very beneficial for answering security questions, opening bank accounts, applying for credit, verifying accounts, among many other things. However, getting this information can be a little tricky, and sometimes unobtainable. With a little luck and this guide, you will have the tools and resources to give you the best chance possible to obtain this information.

We hope you enjoy, Now you may proceed to order..

Stolen Background Check data facilitates cascading breaches against individuals and Critical Infrastructure organizations instead of against irresponsible Data Brokers. For instance, an attacker can leverage Background Check information to compromise a target's security questions on other accounts and continue to laterally compromise accounts and systems until the target cannot be further exploited or until a critical infrastructure system is compromised.

Dun & Bradstreet, LexisNexis , and Kroll Background America

In 2013, security researcher Brian Krebs conducted a seven month investigation into the breach of three major data brokers. A now defunct domain, exposed[.]su, published the social security numbers, birth records, and credit/ background reports on First Lady Michelle Obama, CIA Director John Brennan, then-FBI Director Robert Mueller, Bill Gates, Beyoncé Knowles, and other prominent public figures. The information had been exfiltrated by the hacktivist group UGNazi in 2013 from an underground cybercrime identity theft service called ssndob[.]ms, which had acquired the information through a small, but potent botnet of at least five infected systems at several large United States consumer and business data brokers, including Dun & Bradstreet (2 infected servers) in Short Hills, N.J., LexisNexis (2 infected servers) in Atlanta, and Kroll Background America (1 infected server), managed by Altegrity, a holding company in Falls Church, VA. [27].

In summer 2013, SSNDOB was compromised by cyber attackers and its database was stolen. Copies of the data indicate that approximately 1,300 users spent hundreds of thousands of dollars (at prices ranging from \$0.50 to \$2.50 per record, and from \$5 to \$15 for credit and background checks) to access the information contained in a database of over 4 million

Americans. The exfiltrated database indicated that between early 2012 and mid-2013, the service delivered more than 1.02 million SSN's and 3.1 million date of birth records, and thousands of background reports, to malicious threat actors with (likely proxy-ed) Internet addresses registered in the United States, Russia, and the UK. SSNDOB also licensed its system to at least a dozen high-volume threat actors, likely cybercriminal organizations, who were provided with application programming interfaces (APIs) that facilitated direct and transparent lookups through SSNDOB. [27]

The online botnet dashboard on the LexisNexis systems indicated that a malicious file, "nbc.exe", infected the two public facing servers on April 10, 2013. The Dun & Bradstreet servers were similarly compromised on March 27, 2013 and the final server located at an internet address assigned to Kroll Background America, Inc. was compromised in June 2013. The three data brokers were targeted by identity thieves for the PII (demographics) and for the consumer and business habit and practice data (psychographics) contained on their servers. Among this information was knowledge-based authentication (KBA) information that credit services use to verify applicants' identities [27].

The same cyber-adversaries also compromised systems belonging to the National White Collar Crime Center (NW3C) on May 28, 2013 [28]. The attackers appear to have exfiltrated 2.659 million consumer complaint forms from the Internet Crime Complaint Center (IC3) from May 8, 2000 to Jan. 22, 2013. The complaints would not be very useful for identity theft, but could be leveraged in a spamming or spear-phishing campaign. The attackers also searched through records related to ongoing civil and criminal cases, searched systems for lists of foreign law enforcement agents who were assisting in active criminal cases, and forced databases to dump information from the law enforcement agents acting in a supervisory role at the NW3C [28]. It is possible that this information was useful to cybercriminals to avoid law enforcement or to nation state entities.

LeapLab and Co-Defendants (2014)

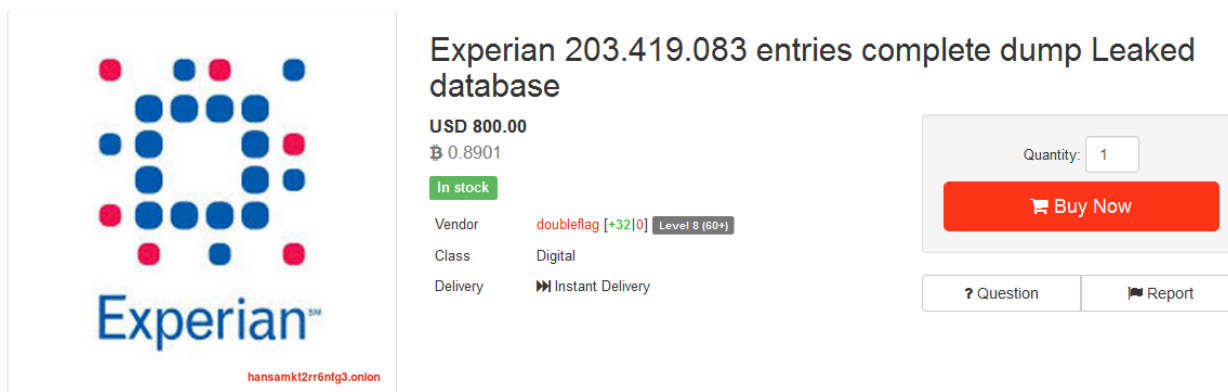
In 2014, the FTC filed charges against Sitesearch Corporation (formerly LeapLab) and the other Co-Defendants citing charges of unfair trade practices in violation of Section 5 of the FTC Act, relating to the illicit sale of consumer personal and financial information. On February 18, 2016 the FTC settled a dispute with LeapLab LLC and other Co-Defendants, who knowingly sold consumer information (Social Security numbers, bank account details, etc.) to third parties, who employed this information for illicit purposes. The information was obtained from short-term payday loan applications provided by candidates on the Co-Defendants' websites. The Co-Defendants then knowingly sold the applications to scammers, telemarketers, and other non-lenders who abused the data. One client third-party, Ideal Financial Solutions, made unauthorized debits (totaling \$4.2 million) from consumers' bank accounts [29].

Experian (2011, 2015)

In November 2011, a cybercriminal identity theft service, Superget[.]info and findget[.]me began marketing “fullz” (Social Security numbers, name, address, place of work, mother’s maiden name, email accounts, passwords, birthdays, driver’s license records and financial information) on half a million Americans, to Deep Web buyers. The information was obtained through Court Ventures, a data broker that was acquired by Experian, one of the three credit agency data brokers, in March 2012. Hieu Minh Ngo, the 24-year-old Vietnamese proprietor of Superget[.]info gained access to Experian databases by posing as a U.S. based private investigator. Ngo gained access to personal and financial records on over 200 million Americans, despite paying for his monthly access to Experian with wire transfers from Singapore. Ngo was arrested by the United States Secret Service in 2013 [19].

In October 2015, Experian revealed that its systems had been compromised and the information of 15 million customers who had applied for “T-Mobile USA postpaid services or device financing from September 1, 2013 through September 16, 2015”, may have been exposed. The compromised information included names, addresses, Social Security number, driver’s license details, and passport numbers [30].

Figure 17: Perpetual Breaches of Experian Exemplifies Data Brokers' Inability to Secure Consumer Data



Experian 203.419.083 entries complete dump Leaked database

USD 800.00
₮ 0.8901

In stock

Vendor: doubleflag [+32|0] Level 8 (60+)
Class: Digital
Delivery: Instant Delivery

Quantity: 1

Buy Now

? Question Report

hansamkt2rr6nfg3.onion

Listing Details

Experian complete dump 203.419.083
(THIS DATABASE NEVER BE A PART OF ALL LEAKED DATABASE PACKAGE)

have this field

FIELD DESCRIPTION

FIRST NAME

MI

LAST NAME

PREFIX

ADDRESS

SUITE/APT

CITY

STATE

ZIP5

ZIP4

DELIVERY POINT BAR CODE

FIPS STATE CODE

FIPS COUNTY CODE

LATITUDE

LONGITUDE

ADDRESS TYPE INDICATOR

0 = Undetermined

1 = Single Family Dwelling

2 = Apartment with unit designator

3 = Apartment without unit designator

4 = Rural Route

5 = Post Office Box

COMMUNITY REINVESTMENT ACT (CRA) INCOME CLASSIFICATION CODE

1 = LOW INCOME

2 = MODERATE INCOME

3 = MIDDLE INCOME

4 = HIGH INCOME

Figure 17 is of a 2016 Hansa Market listing of exfiltrated Experian database information. Some of the exfiltrated fields are provided. This data trove is the third Experian breach detailed in this blogpost, but there were likely countless other incidents and breaches that were not discovered in our research. The other major credit unions and the data broker community likely implement similar information security as Experian. With these databases, an adversary could launch attacks on financial markets, could identify societal triggers for information warfare, etc.

Problem 3: Collected Data Can Easily Be Leveraged to Manipulate Population Perception

Operators utilize the information collected by data brokers in order to exert some level of influence over one or more subsets of the population. Most operators are marketing firms, political campaigns, and other organizations who are trying to better connect with the general public; however, cyber-adversaries and other threat actors can exfiltrate or purchase (via an intermediary) the same data and employ the same methodology to tailor focus their malicious campaigns to specific population subsets. If the data are granular enough, if the data steward failed to sufficiently anonymize the data, or if the adversary obtained the data prior to anonymization, then cyber threat actors can leverage data sets to precision target average users, government personnel, high-value users, or critical infrastructure organizations.

Figure 18: Government Sites May be Targeted in Data Disclosure Attacks Meant to Influence Public Perception

Forums / Fraud Related & Services / I have root to .gov and .edu websites what should i do?

I have root to .gov and .edu websites what should i do?
submitted 4 months ago by killabill

As the title says i recently got root in some different .gov and .edu websites. But i dont know what i could do with them from there.

Any suggestions would be highly appreciated

[Reply](#) [Subscribe](#) [Report](#)

justmoja [71] 2 points 4 months ago
you can put urls on the website that you have and got paid .
if you are interested pm me
[Reply](#) [Report](#)

sybergryme [6] 2 points 4 months ago
Killabill Can you PM me I have questions regarding root you got. I think you could be a big help.
[Reply](#) [Report](#)

Fun-guy [2] 2 points 4 months ago
people will buy URL's placed on the sites for seo purposes, depending on their metrics. Can charge decent prices for good edu and gov sites
[Reply](#) [Report](#)

jdutchman [Vendor] [549] 3 points 4 months ago
Go to their drives through panels download all there data see if you could get some delicious info sell or use then deface it make yourself famous
[Reply](#) [Report](#)

killabill [11] [OP] 2 points 4 months ago
Yes i was thinking about that but i wanted to know whether using it as an email, or any other use of the domain would be a waste of time?
[Reply](#) [Report](#)

JesusMalverde [Vendor] [16] 3 points 4 months ago
Possibilitys are almost endless...
Of course you can use the .edu mail addresses to get some benefits like free amazon prime or different microsoft products and much more for free or just sell .edu/.gov mail accs.
Even spamming/phishing would be a possibility from both of them, but always take care of your security and dont get yourself busted.
[Reply](#) [Report](#)

killabill [11] [OP] 2 points 4 months ago
Ah seems very cool, thx :)
[Reply](#) [Report](#)

JesusMalverde [Vendor] [16] 3 points 4 months ago (Last edited: 4 months ago)
On second thought... may I can help you selling the .gov mail addresses.
If you interested take a look at my vendorpage for contact information.
[Reply](#) [Report](#)

Figure 18 captures a Hansa Market conversation on the use of compromised .gov and .edu sites. One user recommends exfiltrating sensitive data and defacing or exposing it in embarrassing data dumps. These activities increase renown in script kiddie communities; however, they are also the most basic form of information warfare. Public disclosure of sensitive information can devastate any target. Psychographics can be used to develop fake news, disinformation, etc. that incorporates just enough sensitive information to seem credible. Alternately, the data could be sold to sophisticated adversaries for use in their psychographic analyses or multi-vector information warfare campaigns.

While there are different approaches, one standardized methodology of influencing a population begins by defining broad objectives, by planning a communication strategy, and by identifying self-identifying audiences and social groups. Behavior and attitudes determined by social context are more monolithic and can be more easily triggered; therefore audiences can be more reliably predicted and influenced based on self-defined categories (e.g. devout Christian) rather than imposed categorization (e.g. all women). Next, the operator employs polls, field research, and other analytical methods to determine what conditions might alter the behavior of an audience and which triggers have the greatest impact on altering audience behavior. The triggers are used to develop an Intervention strategy, which could include social media campaigns, tailored banner advertisements, news/ fake news articles, etc. The intervention strategy is used to dictate and direct the actions of the population subset. Finally, the operator defines and collects metrics to measure how effectively the strategy achieves campaign objectives. This feedback can be fed into purchased or developed data analytic dashboard tools in order to automatically optimize the stratagem and decisions of the campaign in real time, according to changes in audience attitudes, fears, opinions of current events, etc. [31]. An operator can even use multiple dashboards to analyze multiple populations or to predict the behavior of target users under different conditions.

Cyber Adversaries Weaponize Psychographic Data for Precision Targeted Attacks On Critical Infrastructure Executives and Organizations

Since the very first data exfiltration of the very first cyber-breach, malicious adversaries have obtained, exploited, and weaponized demographic information to repeatedly harass victims. Some data, such as names, birthdays, etc. can be used to answer security questions or to otherwise obtain privileged credentials that enable cascading incidents. Other data, such as healthcare EHR or financial PII can be exploited for identity theft or sold to cybercriminals. While tedious and difficult, these potential outcomes are well-documented and some risks can be mitigated through mitigation strategies such as credit freezes.

Though a few sophisticated adversaries were prescient, the vast majority of cyber threat actors are only beginning to realize the potential of leveraging psychographic data over demographic data in multi-vector hybrid attacks against high-value targets such as C-level executives, niche-personnel, or critical infrastructure. The aforementioned attacks that yield demographic data can be lucrative and useful for identity theft, but they are less attractive to an adversary that is not financially motivated, such as a nation-state adversary, because for the most part, demographic data can only be used to steal identities, monetize assets, or to further exploit un-cyber-hygienic victims. Alternately, psychographic data enables the attacker to launch numerous cascading incidents that exploit the specific behavioral patterns and psychology of explicit population segments in order to effortlessly entice targets to bypass their own

cybersecurity and cyber-hygiene defenses, and to thereby self-victimize and welcome the adversary onto their network.

Psychographic data are not difficult for an adversary to obtain and weaponize. The gross negligence and systemic greed of data broker firms, as demonstrated in the sample above, guarantees that at least one broker, out of the hundreds, would always be willing to knowingly or unknowingly sell an adversary psychographic data and the data analytic software to manipulate that information. Alternately, attackers could breach data broker servers, data broker client servers, or the servers of practically any company, in order to obtain the initial psychographic data necessary to launch precision targeted, cascading attacks. The vast majority of users remain unaware of the swath of corporate dragnet surveillance that records their every web search, categorizes their every email, monitors their every financial transaction, etc. As a result, when an adversary breaches a corporation and exfiltrates psychographic data, there is nothing that potential victims can do except wait to be eventually compromised as their every online activity becomes a potential point of compromise.

Targeted Psychographic Attacks are Evolving

Adversarial cyberattack campaigns that utilize psychographic data analytics can devastate average users, high-value targets, and critical infrastructure sectors, because this bleeding-edge attack vector enables adversaries to precision target select population segments with tantalizing, victim-tailored lures, in order to coerce targets into self-victimization; thereby, bypassing cybersecurity and cyber-hygiene controls, and granting the adversary carte-blanche access to critical networks and to treasure troves of high-value sensitive data. The data can be further exploited in cascading breaches against additional targets and against critical infrastructure. The use of psychographics in attacks will proceed as complex multi-vector campaigns incorporate disinformation, propaganda, real and fake news lures, malvertising, spear-phishing emails, and watering-hole attacks. The intent of the campaign is to bombard targets within the select population segment (for instance, niche- Energy sector personnel, Financial sector C-level executives, etc.) with enough disinformation, propaganda, and news/fake news based lures, to subtly alter the targets' perception of reality to the extent that for one reason or another (trust, curiosity, incredulity, etc.) they lower their mental inhibitions and act in the moment to respond to at least one of the lures.

In a psychographic attack, an adversary needs to engage with a data broker willing to sell the data set (to a spoofed or nation-state owned organization) or the attacker needs to identify the steward of the desired data and bait their personnel into accepting a lure that facilitates the installation of malware on the system. The lure may be a generic phishing campaign or a more sophisticated breach. Similarly, the sophistication of the malware or exploit kit employed is dependent on the adversary. More sophisticated threat actors will conduct multi-vector

campaigns that incorporate ransomware, launch distributed denial of service attacks, or that infect the victim's systems with botnet or rootkit malware. These auxiliary attacks obfuscate the data exfiltration, distract organizational resources, and mask the indicators of compromise that could be used to identify the specific attacker. Finally, the threat actor needs to purchase or develop a data analytics platform capable of discerning meaningful trends in the dataset. Artificial intelligence systems and sophisticated database management solutions will likely be included due to their convenience and utility in the tabulation and manipulation of the data.

After an adversary has analyzed psychographic data and determined a trigger or initial attack vector, they need to select an effective delivery mechanism that will facilitate the installation of malware that can exfiltrate data or that can record keystrokes, capture screen shots, activate the microphone and cameras, etc. At the start of a campaign, disinformation and propaganda can serve as a lure or it can help the adversary identify contentious topics and vulnerable information streams within a community. Further, disinformation and propaganda can be used to subtly shift community focus and conversations or to desensitize and inundate a population segment to the point that their cybersecurity and cyber-hygiene defenses are whittled down and their mental inhibitions are lowered. Real and fake news are attractive lures because the victim's curiosity, incredulity, or carelessness tantalizes them, with little effort on behalf of the attacker. Malicious real and fake news lures are articles about current events or polarized topics that are titled in such a way as to draw in un-cyber-hygienic readers. Victims spread malicious news and fake news lures to their social and professional networks. Additionally, attackers occasionally weaponized technical documents and whitepapers with malware in order to precisely target only members of a select field, such as cybersecurity.

Figure 19: Malvertising Can Deliver Malware From Legitimate Webpages

Guaranteed AdSense Approval - Step by Step

Vendor [debuyerking](#) (3367) (4.88★) (🔗 782, 4.92/5)
 (👤 1043/19/23) (✈️ 500~700, 4.92/5) (M #257, 9.86/10) (🔥 1509/30/30)
 (🌱 172/100) 🟢

Price ₪0.001168 (\$1)

Ships to Worldwide, Worldwide

Ships from Worldwide

Escrow Yes




Product description

how to get Guaranteed AdSense Approval - Step by Step

The Deep Web guide offered in the Hansa Market listing captured in Figure 19 claims to enable malvertising threat actors to get automatic Google AdSense approval. AdSense serves approved targeted advertisements to specific audience based on psychographic profiles. By subverting the AdSense verification process, malvertisers can target select communities such as critical infrastructure niche personnel, corporate executives, etc.

Malvertising (Malicious Advertising) is perhaps the most alarming and the most effective potential attack vector for psychographic campaigns. Consider that there are two basic types of sites, malicious sites and innocuous sites. Malicious sites lure visitors and infect their systems with malware. The link to the site is usually the lure, which might be cleverly titled, might offer something free, or might just be a misspelled variation of a legitimate site (i.e. Google instead of Google). Innocuous sites are the well-curated everyday sites operated by non-malicious organizations and individuals. Adversaries sometimes try to digitally compromise these sites to infect them with malware; however, basic cybersecurity measures typically prevent or mitigate most attempts before any harm reaches visitor's systems. Malvertising attacks enable cyber adversaries to infect users' computers with malware, without requiring the adversary to lure the user to a malicious site and without any need to compromise legitimate sites. Every time a user visits any site, nano-second and micro-second background processes in their computer, browser, on the Internet Provider servers, etc. connect to various parts of the internet to load different parts of the desired web page. To the user, this all appears seamless (though there are still times when part of a webpage fails to load and the user has to refresh the page). Advertisements are one category of the page that loads separately. Cyber attackers have begun either compromising advertiser sites or outright purchasing advertisement spots from legitimate ad networks and submitting malicious advertisements. Some malicious advertisements only install malware if the user clicks on the advertisement; however, others exploit pixels, iframes, cookies, and other technical background Internet components to install malware onto the system of any user who visits a page displaying the malicious advertisement. Malvertising enables psychographic attackers to poison the banner advertisements on popular sites, to load innocuous newsletters with malware, or to lure unsuspecting targets to watering-hole sites with tailored ads offering accreditation, software, niche-specific information or products, etc. In short, once an adversary has the psychographic data to target a specific community through multi-vector attacks, the success of the campaign is only a matter of time.

Figure 20: Script Kiddies are Already Toying with Psychographic and Demographic Information Warfare



The Underground Collection 23.09.2016

20,000 Items | 13k cardable (sql) sites, 300k Steam Acco

USD 5.00

฿ 0.0056

98 in stock

Shipping options

digital [Next Day] [+ USD 0.00]

Vendor **Littlecube1** [+3|0] Level 1 ★ Trusted Vendor

Class Digital

Quantity:

[Buy Now](#)

⚠ Please make absolutely sure the URL inside the product image matches the one in your browser! If they do not match, leave this site immediately.

♥ Favorite ? Question 🚩 Report

Listing Details

May you use this collection to garner interest and curiosity in the field of technology. To not only play defensively, but to also play offensively! That's where the real fun begins.

In just the past few years, we have seen hacking and leaking activities reach revolutionary levels around the world. The new generation of people practicing these dark arts (or light, depending on how you view it) have shown us that corporations CAN feel the burn and that people CAN do something about it. With enough creativity and imagination, hacking can be one of the most powerful, potent, and most importantly, fun skills you can have at your disposal. This is the Underground Collection Part 1.

You can read all the guides you want on how to make money, but this is all the stuff you need to make REAL money. Most people in this world are up to their eyes in debt, go to work every day to pay of tiny bits of that debt, and most likely die leaving their children debt. There is a solution though: take your power back.

FUUUUUUAAAARK BRAH'S bumpin that sickKunt music as we speak!

Some of the websites in the vulnerability list are very juicy, for example:

[+] <http://orc.scripts.mit.edu/people/student.php?name=stgoh> (SQLi)

[+] <http://www.eeweb.ee.ucla.edu/Biography2.php?displayid=143> (SQLi)

[+] http://www.nationalgridus.com/aboutus/a3-1_news.asp?SiteID=1 (SQLi)

[+] <http://tokenbooks1ma.cityoflondon.gov.uk/search/BookTranscription.php?BookNumber=1337> (SQLi)

[+] <http://www.laptopmania.co.uk/products.php?cat=> (SQLi)

[+] <http://www.tabletpadshop.co.uk/products.php?cat=> (SQLi)

[+] <http://www.fujitsulaptop.co.uk/products.php?cat=> (SQLi)

[+] and many, many more

I put some from my personal stash in with the big list. So consider it a gift :)

This is what you'll be paying for:

Source Codes and Builds:

[X] Ransomware (uncompiled) (3 versions w/ changelogs)

[X] Botnets (338)

[X] Exploit Kits (Crimepack, Bleedinglife, Sakura, Firepack, Icepack, Phoenix, etc.) (11)

[X] Banking Trojans (9)

[X] POS (point of sale) Malware (3)

[X] Rats (11)

- [X] Binders (15)
- [X] DDOS'ers (3)
- Tutorials:
 - [X] A LOT of carding tutorials
 - [X] Exploiting Reflective XSS
 - [X] Creating your own secure TOR hidden service
 - [X] How to spy on cellphones
 - [X] A CyberPunk's guide to dumpster diving
 - [X] ISP Doxing (employee method)
 - [X] The holy grail of DOXing
 - [X] Changing payload signatures (etc.)
 - [X] LFI/RFI/XSS/SQLi exploitation etc.
 - [X] Staying anonymous
 - [X] Social Engineering
 - [X] Shelling web servers etc.
 - [X] Cloudflare Unmasking
 - [X] Rootkits and rooting servers
 - [X] Preventing persona contamination
 - [X] Literally every resource to become a fucking skilled h4ck3r
 - [X] A LOT not listed here
- Scripts:
 - [X] All the scripts from the infamous Dark0de forum (now defunct, lol Rory)
 - * Many categories not listed here (481 scripts - good pwnage potential)
 - * Custom Scanners
 - * Bruteforcers
 - * Bot Killers
 - * Encryption Scripts
 - * Database (extraction, scanning, etc.)
 - * Scripts written in C, perl, ruby, etc.
 - * A LOT more cripts

- [X] A TON of google dorks for different exploits
- SOCKS and Proxies:
 - [X] SOCKS and proxies in almost any country (1800+)
- Free Stuff:
 - [X] 300k+ steam accounts
 - [X] Over two million emails for spamming purposes
 - [X] Social security numbers and DOB's
 - [X] .6gb E-Whore Collection (biggest to date)
 - [X] 4000+ updated onion sites (warning: some may be graphic)
 - [X] 13k vulnerable websites
 - [X] 150k+ hacked emails/passwords
 - [X] 5GB of programming resources
 - [X] 30 million word wordlist
 - [X] File upload vulnerability .gov edition
 - [X] Global Government IP Ranges
 - [X] Personal Stash of vulnerable sites (JUICY)
 - [X] More cardable sites
 - [X] Phrack e-zine collection
 - [X] 500+ hacked facebook accounts
 - [X] 500+ private shells
 - [X] A LOT of porn accounts
 - [X] Fresh emails for paypals
 - [X] Databases (JUICY)
 - [X] PHP mailers
 - [X] SSH tunnels and SOCKS
 - [X] Some freebie CC's
- [X] Changing Images Of Man - Stanford Research Institute
- [X] COINTELPRO Techniques for dilution
- [X] Communist Psychological Warfare
- [X] Cult Psychology and Brainwashing
- [X] Do Political Protests Matter
- [X] Eight Traits of the Disinformationalist
- [X] From memory societies to knowledge societies
- [X] Gestalt Bubble
- [X] Get Anyone to Do Anything - David J. Lieberman
- [X] How to Spot a Spy
- [X] How To Win Friends And Influence People
- [X] Individual Deception and Coercion
- [X] Industrial Society And Its Future
- [X] Infomation as Communication Disease
- [X] Instincts of the Heard in Peace and War
- [X] Military
- [X] Neuro Linguistic Programming
- [X] No Tech Hacking - A Guide to Social Engineering
- [X] Prometheus Rising
- [X] Propaganda (by Bernays)
- [X] Removing Knowledge
- [X] Resistance And Persuasion
- [X] Ritual as Language
- [X] Seventeen Techniques for Truth Suppression
- [X] Silent Weapons for Quiet Wars
- [X] Simulacra and Simulation - Jean Baudrillard
- [X] Social Engineering - the Art of Human Hacking
- [X] Strategic Information Warfare
- [X] Subversion of Social Movements by Adversarial Agents
- [X] Terrorism
- [X] The Advertised Mind
- [X] The Age of Manipulation - Wilson Bryan Key
- [X] The Art of Deception
- [X] The Art Of Memetics
- [X] The Byzantine Generals Problem
- [X] The Crowd - Gustave Le Bon
- [X] The Medium is the Massage - Marshall McLuhan, Quentin Fiore
- [X] The Parallax View - Zizek
- [X] THE POWER OF PERSUASION How We're Bought and Sold - Robert Levine
- [X] The Psychology Of Entertainment
- [X] The Selfish Meme
- [X] The Soros Media Empire - Michael Baker
- [X] The System Explained
- [X] The topology of covert conflict
- [X] Think Two Products Ahead
- [X] Trigger Words and How They Are Used Against Us
- [X] Twenty-Five Rules of Disinformation
- [X] Understanding Media - the Extensions of Man - Marshall McLuhan
- [X] You Are Being Lied To
- [X] Deception Research Program No 9
- [X] Principles of Counterdeception
- [X] Psychology of Intelligence Analysis
- [X] Brainwashing Manual - Synthesis of the Russian Textbook on Psychopolitics - L Ron Hubbard
- [X] The Battle For Your Mind, by Dick Sutphen
- [X] Interrogation
- [X] Reprogramming
- [X] CIA - Human Resource Exploitation Training Manual (1983) - aka Honduras Manual - a1-g11 (Torture)
- [X] Educing Information
- [X] FM 34-52 Intelligence Interrogation
- [X] KUBARK
- [X] CIA Kubark 1-60

The listing depicted in Figure 20 indicates that script kiddies now recognize the potential of information warfare and Big Data analytics. Databases, guides to disseminating propaganda, and other information warfare components are offered in this low –level market listing. Considering that most of the data, tools, and techniques offered are likely outdated, it begs the question: What tools, techniques, and procedures are more sophisticated adversaries now using in their attacks?

Psychographics Enable Tailored Sector Specific Attacks

The employment of psychographic data analytics is limited only by the creativity of the adversary. Any pool of data large enough to conduct data analytics will have the potential to enable attack campaigns that can be used to infect more systems and exfiltrate additional data pools. For instance, say an adversary breached a low-level, third-party company that produced spreadsheet, payroll, or other management software. The adversary could leverage stolen usage and feedback data to develop a compelling lure and then target any client, in order to laterally compromise Human Resources or payroll departments, in practically any critical infrastructure segment. Similarly, if an attacker wanted to target a high-value, siloed critical infrastructure population, such as Energy sector SCADA and ICS administrators, then the attacker could leverage psychographic data to discover what interests, concerns, and web-browsing habits, were shared among the greatest cross section of potential victims. Next, the adversary would distribute spear-phishing emails (by weaponizing newsletters and mailing lists), real and fake news lures and watering-hole links. They would also place malicious advertisements on popular niche sites, on the site of accreditation authorities and members societies, on the site of academic journals, etc. In either scenario, if the adversary has enough data to generate the lures, but lacks the target list, then the adversary can compromise sites where population segments willingly self-identify or list their professional information, such as LinkedIn, professional job sites (Monster, Indeed, etc.), or executive recruiting organizations. These services can also be exploited to identify and target high-value individuals, such as system administrators or C-level executives.

Psychographics Facilitates Personalized Attacks Against High-Profile Individuals

Individual, high-value targets can be manipulated, targeted, or exploited through the information contained in broad psychographic data sets (to predict behavior, generate lures, etc.) or in granular, de-anonymized sets. Consider that the healthcare industry collects a significant amount of data on every patient, that much of the collected information is gratuitous, and that the vast majority of data subjects remain unaware that their healthcare network is generating additional revenue by selling the data contained in their EHR, to indistinct third-parties. Healthcare organizations have become data brokers to pharmaceutical, research, and other organizations by selling collected data without providing significant notice or choice to hospitalized and vulnerable individuals. This sectoral development is troubling considering that the healthcare sector is a frequent target of cyber-attackers aimed at exfiltrating their vast treasure troves of EHR data [32]. In fact, the high-profile Anthem breach resulted in the exfiltration of 78.8 million EHRs, which is approximately a quarter of the U.S. population. Given the amount of healthcare data already exposed due to a lack of fundamental cybersecurity and basic cyber-hygiene, privacy and security advocates should be concerned about how psychographic data can be combined with anonymized or de-anonymized electronic health

records in personalized attacks against high-profile individual or in societal attacks that target a specific region or healthcare network.

Portions of the de-identification provisions within the 2003 Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule were developed as the results of the 1997 re-identification of Massachusetts Governor William Weld from medical data contained within an insurance data set which had been stripped of direct identifiers, using a voter registration list from Cambridge, MA. In all likelihood, Weld was only re-identifiable because he was a public figure who experienced a highly publicized hospitalization [33]. Nevertheless, since then, privacy advocates have repeatedly proven the possibility of de-anonymizing healthcare data and matching it to specific patient records. For instance, a \$50 health data set sold by the State of Washington was cross referenced with 2011 newspaper stories of hospitalizations, and 35 out of 81 cases (43 percent) were accurately re-identified. The data set contained patient demographics, diagnoses, procedures, attending physicians, hospital information, a summary of charges, and how the bill was paid. It did not contain patient name or addresses. The data set was available for purchase to the general public [34]. Evolving data mining and data analytics techniques make the de-anonymization of data increasingly trivial.

One popular concept of anonymizing data is k-anonymity, which states that each record in a dataset is indistinguishable from at least k-1 other records, with respect to identifying attributes. However, if the dataset lacks diversity or if the attacker has background knowledge of the data subjects, then the data can be de-anonymized [35]. K-anonymity is being slowly phased out by more secure models; however, many privacy regulations, guidelines, and methodologies are still based on it. As a result, datasets are often insufficiently secured against attacks that could allow for the re-identification of specific individuals, provided that the attacker possess some prior information about the target (i.e. they have pre-identified their target, know that the individual is in the data set, and have collected basic information about them from public sources such as social networks).

Once a high-profile target had been identified and profiled, the adversary can tailor personalized lures. For instance, the attacker could spoof a medical bill, could send them a surgically precise urgent email about a medication for their condition, etc. Alternately, the adversary could release sensitive data to denigrate the individual, to devalue a company through public embarrassment, or to cause any number of personal or societal harms. In demonstration of how easy it is to target high-profile targets, one researcher consulted two cybercrime identity theft services that had data from compromised data brokers, and was able to obtain the full address history and social security numbers of all 13 members of the U.S. Senate Commerce Committee Subcommittee on Consumer Protection, Product Safety and

Insurance, of the head of the Federal Trade Commission and of the head of the Consumer Financial Protection Bureau [36].

Russia Continues to Masterfully Conducting Information Warfare Campaigns

Psychographic data does not have to be used to facilitate the exfiltration of information in additional breaches. Because psychographic attacks begin with the identification of triggers and polarizing categorizations through Big Data analytics, the attack vector can also be used in information warfare attacks intended to promote uncertainty, incite divisiveness, or undermine a political system. The repeated exposure to disinformation, propaganda, or inaccurate information (i.e. fake news), desensitizes the target and eventually, some of the population may be persuaded to believe the false information [37]. A more sensational lure causes more people to pay attention to it and therefore convinces more people to believe it. If the material is convincing enough, then leaders and the media may even begin disseminating it and evangelizing it; thereby, simulating a layer of credibility. The remainder of a population, who are either ignorant of the lure or who consciously object to the subject matter, are polarized against those deceived by the lure. Russia is well known for this form of manipulative information warfare campaign. Russian APTs often spoof their lures or indicators of compromise to mimic other groups or political entities. Russia even had, and likely still has, a foreign propaganda division, known as "The Agency," that is tasked with disrupting foreign nations through internet "trolling" and digital-information warfare [38]. Unclassified reports from the FBI, DHS, and DNI indicate that Russia may have engaged in information warfare against the United States during the 2016 Presidential election, through the dissemination of disinformation, propaganda, and fake news. The DNI report states "We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency." The report further concluded that this activity "followed a longstanding Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'" Finally, the report indicated that the information warfare campaign may have been multi-vector and may have involved demographic and psychographic data that was obtained in previous APT attacks, saying "The Kremlin's campaign aimed at the US election featured disclosures of data obtained through Russian cyber operations; intrusions into US state and local electoral boards; and overt propaganda. Russian intelligence collection both informed and enabled the influence campaign." In this instance, Russia focused on information related to U.S. political parties, think-tanks, and lobbying groups, that had the ability to shape future U.S. policy. DNI assesses with high confidence that disinformation, propaganda, and fake news from the Russian GRU was disseminated through the Guccifer 2.0

persona, DCLeaks.com, and WikiLeaks. The latter was used due to its notoriety. It is likely that Russia will continue to evolve and to perfect this brand of information warfare that utilizes demographic and psychographic data, in future campaigns against the United States and other foreign powers. The DNI agrees with this assessment, stating, "We assess Russian intelligence services will continue to develop capabilities to provide Putin with options to use against the United States, judging from past practice and current efforts. Immediately after Election Day, we assess Russian intelligence began a spear phishing campaign targeting US Government employees and individuals associated with US think tanks and NGOs in national security, defense, and foreign policy fields. This campaign could provide material for future influence efforts as well as foreign intelligence collection on the incoming administration's goals and plans" [39].

China is Already Collecting Data to Manipulate Key Industries and Critical Infrastructure Executives

Nation state threat actors gain the greatest advantage and utility from the employment of psychographic attacks in multi-vector, hybrid information warfare campaigns, designed to cause socio-economic or geopolitical intractability, to exfiltrate intellectual property, to target high-value assets, or to victimize an unsuspecting general population. China conducts cyber and information warfare operations in support of its Thirteenth Five-Year Plan, against foreign nations, through its numerous nation-state sponsored advanced persistent threat groups that comprise its Third Department. Further, every organization operating in China employs at least one mandatory Chinese government liaison, which has full access and authority to examine software, alter products, and influence organization decisions. An organization that operates in both the United States and China could easily be compromised to provide psychographic information to the Chinese government. Even if the organization did not knowingly share the information, the linked databases and systems or an insider threat, could be used to transfer the data. The information could then be passed to the numerous APT groups to facilitate future breaches or it could be combined with other exfiltrated information in the development of complex dossiers on Americans for espionage purposes. Recent cascading breaches, perpetrated by Chinese APTs indicate that China already appreciates the value and utility of combining demographic and psychographic information.

The New War Against OPM Victims Has Begun

In 2014 and 2015, the Chinese sponsored Deep Panda APT conducted "THE" cyber-Pearl-Harbor with their two breaches of the United States Office of Personnel Management (OPM). The granular information contained in the 127 page SF-86 forms was demographic and psychographic in nature and the data will compromise United States Intelligence assets and will victimize its critical infrastructure personnel and general population for decades.

Deep Panda (also known as Black Vine or Pupa) predominantly targets the U.S. Healthcare, Aerospace, Energy and Government sectors, with watering hole attacks; zero-day exploits, and spear phishing campaigns that incorporate an exploit kit consisting of the Sakurel Trojan, the Hurix Trojan, and the Mivast backdoor, and tools from the Elderwood platform. Deep Panda may be affiliated with Topsec, a Beijing IT firm that focuses on information security research, training, auditing, and security products. The threat actor has access to significant resources that have enabled it to conduct multiple simultaneous campaigns against United States Federal government agencies and major western health care providers for extended time periods. In the United States health care sector, Deep Panda has breached Anthem (78.8 million EHR), CareFirst (1.1 million), and other providers. In June 2015, DHS, FBI, Congress, and the public were informed that the Office of Personnel Management's (OPM) systems were breached by an adversary, believed to be the Chinese nation state APT Deep Panda, in November 2013, March 2014, and October 2014. The breaches resulted in the exposure of the personal information contained in the SF-86 forms of 22.1 million current and former United States Federal employees. 5.6 million finger-print files were also stolen. The attribution was based on the malware discovered on the system and the tactics and procedures employed in the attack. Deep Panda also breached United Airlines in 2015 and stole departure and destination records [40].

Figure 21: Compromised Travel Information Provides Psychographic Data Capable of Harming Businesses, Individuals, and Intelligence Operations




★ Courvoisier ★ OG CHEAPEST British Airways Accounts with Avios Points + DOB ★

★ Introduction ★ ----- Get your material from the SOURCE, not the wannabes. Greetings everyone, this listing is for the advertisement of hacked British Airways accounts. I'm the original, first vendor to sell these accounts, I have truly unlimited stock, all these fake wannabe vendors are consistently popping up trying to copycat my listings and compete with my p...

Sold by **Courvoisier** - 3629 sold since Apr 10, 2015 Vendor Level 1 Trust Level 7

Features		Features	
Product class	Digital goods	Origin country	United Kingdom
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

Minimum 10,000 Points - 1 days - USD +3.66 / item

Purchase price: USD 0.00

Qty: Buy Now Buy Now

0.0000 BTC / 0.0000 XMR

Product Description

★ Introduction ★

Get your material from the SOURCE, not the wannabes.

Greetings everyone, this listing is for the advertisement of hacked British Airways accounts.

I'm the original, first vendor to sell these accounts, I have truly unlimited stock, all these fake wannabe vendors are consistently popping up trying to copycat my listings and compete with my prices, but the thing is, I fulfill the draughts that occur when these copycats run low on their petty stock, which is why I dominate in this field.

Accounts are supplied with the account holders DOB along with other information with regard to the account.

Learn how to use these accounts to their full potential as you can learn from my "School of Travel 4.0" guide which is also available on my store. This guide will teach you everything you need to know from securing the account to making successful bookings.

★ How are the prices worked out? ★

Current retail price per Avios point: (£0.0056).

Our prices are currently set at (£0.00018) per point.

So you can imagine the amount of money you can save on your trips, right?

I'm presenting the perfect opportunity for you to book your holidays for next to nothing, or perhaps you wish to become a travel vendor and sell bookings yourself to the customers here at AlphaBay? The savings are astronomical. What are you waiting for?!

Figure 21 shows the sale of information similar to the aforementioned airline breach. By psychographically analyzing airline databases, an adversary could gain insight into business dealings, diplomatic relations, critical infrastructure personnel travel patterns, etc. or they could plan cyber-physical attacks that are optimized to result in the greatest impact or harm.

The information exfiltrated from OPM was a catastrophic loss to America, facilitated by gross-negligence, and a lack of cybersecurity regulation and oversight commensurate to the value of the data protected. The full impact of the breach has not yet materialized because the adversary is obfuscating their activities and because they are likely still fine-tuning the data mining and psychographic algorithms necessary to devastate critical infrastructure. In the near future, and for decades to come, this adversary will leverage the data in cascading breaches, espionage campaigns, multi-vector information warfare, and directly against Americans. Every government employee (and their immediate family members) whose information was compromised in the OPM breach has a life of victimization to anticipate. Every email, social media message, text message, etc. that they receive for the foreseeable future is a potential lure from a malicious nation-state APT that possesses 126 pages of granular information about their interests, habits, personality, employment history, proficiencies, failings, vices, etc. OPM provided victims with empty-gesture limited credit monitoring services. Credit monitoring does little to deter identity thieves and it does absolutely nothing to deter APT threats from leveraging psychographic information in multi-vector attacks against specific high-value critical infrastructure personnel (many possessing active clearances). A breach of any one of hundreds of data brokers could have similar implications; yet, data brokers lack even the pitiful cybersecurity and governance that protected OPM.

Conclusion - Information Warfare Leveraging Demographics and Psychographics is the New Normal

For years, consumers have been the subjects of mass dragnet surveillance whenever they used the internet, made a purchase, received medical treatment, etc. After prolonged negligence by data brokers and ignorant data stewards, adversaries now possess massive troves of demographic and psychographic information. Information warfare has developed to include multi-vector attacks that leverage demographic and psychographic data in precision targeted campaigns that utilize disinformation, propaganda, malvertising, social engineering, and real and fake news, as lures to deliver sophisticated malware that exfiltrates data or grants control over the system, to malicious cybercriminals, cyber-mercenaries, or nation-state sponsored advanced persistent threat groups. The tailored attacks made possible through the utilization of psychographic data enables adversaries to victimize Americans who had little notice, knowledge or choice concerning whether their data was collected, if it was used, and how it was protected. As a result, the average consumer is just a victimization case waiting for an adversary. Our critical infrastructure and even American Democracy itself are rendered vulnerable to the manipulations and machinations of cyber adversaries unknown.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: <http://icitech.org/contactus/>

ICIT Websites & Social Media



www.icitech.org



<https://twitter.com/ICITorg>



<https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit->



<https://www.facebook.com/ICITorg>

Sources:

- [1] A. Tanner, "How data brokers make money off your medical records," *Scientific American*, Feb. 2016. [Online]. Available: <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>. Accessed: Jan. 13, 2017.
- [2] A. McDonald and L. Cranor, "The Cost of Reading Privacy Policies," in *I/S: A Journal of Law and Policy for the Information Society*, 2008. [Online]. Available: <https://www.cylab.cmu.edu/files/pdfs/news/CostofReading.PDF>. Accessed: Jan. 10, 2017.
- [3] E. Steel, C. Locke, E. Cadman, and B. Freese, "How much is your personal data worth?," in *Financial Times*, Financial Times, 2013. [Online]. Available: http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4Vqzls6jP. Accessed: Jan. 15, 2017.
- [4] J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini, and R. de Oliveira, "Your browsing behavior for a big mac: economics of personal information online," *Proceedings of the 22Nd International Conference on World Wide Web*, no. 2013, pp. 189–200, May 2013. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2488388.2488406>. Accessed: Jan. 15, 2017.
- [5] S. Mulpuru, "Brief: Digital Touchpoint investments significantly influence US retail sales," in *Forrester Research*, 2016. [Online]. Available: <https://www.forrester.com/report/Brief+US+CrossChannel+Retail+Forecast+2015+To+2020/-/E-RES116715>. Accessed: Jan. 12, 2017.
- [6] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research*, vol. 22, no. 2, pp. 254–268, Jun. 2011.
- [7] L. F. Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice," in *Research Gate*, ResearchGate, 2012. [Online]. Available: https://www.researchgate.net/publication/256041030_Necessary_But_Not_Sufficient_Standardized_Mechanisms_for_Privacy_Notice_and_Choice. Accessed: Jan. 15, 2017.
- [8] R. Gellman, "FAIR INFORMATION PRACTICES: A Basic History," in *Bobgellman.com*, 2016. [Online]. Available: <http://bobgellman.com/rg-docs/rg-FIPshistory.pdf>. Accessed: Jan. 12, 2017.
- [9] "Fact sheet: Plan to protect privacy in the Internet age by adopting a consumer privacy bill of rights," in *White House*, whitehouse.gov, 2012. [Online]. Available: <https://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b>. Accessed: Jan. 15, 2017.

- [10] "Factsheet on the 'Right to be Forgotten' ruling," in *European Commission*. [Online]. Available: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf. Accessed: Jan. 12, 2017.
- [11] "Data Brokers and 'People Search' Sites," in *Privacy Rights Clearinghouse*, 2016. [Online]. Available: <https://www.privacyrights.org/consumer-guides/data-brokers-and-people-search-sites>. Accessed: Jan. 7, 2017.
- [12] S. Ji, W. Li, M. Srivatsa, J. Selena, and R. Beyah, "General graph data De-Anonymization," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 4, p. 12, Jun. 2016. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2894760>. Accessed: Jan. 12, 2017.
- [13] "Data Brokers," in *Privacy Rights Clearinghouse*, 2013. [Online]. Available: <https://www.privacyrights.org/data-brokers>. Accessed: Jan. 10, 2017.
- [14] G. Maus, "How data brokers sell your life, and why it matters," *The Stack*, 2015. [Online]. Available: <https://thestack.com/security/2015/08/24/how-corporate-data-brokers-sell-your-life-and-why-you-should-be-concerned/>. Accessed: Jan. 12, 2017.
- [15] A. Meredith, "How to use Psychographics in your marketing: A beginner's guide," 2016. [Online]. Available: <https://blog.hubspot.com/insiders/marketing-psychographics>. Accessed: Jan. 10, 2017.
- [16] "A Call for Transparency and Accountability" Federal Trade Commission. 2014. [Online]. Available: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> Accessed: Jan, 9, 2017.
- [17] P.-O. Dehay, "Microtargeting of low-information voters," *Medium*, 2016. [Online]. Available: <https://medium.com/@pdehay/microtargeting-of-low-information-voters-6eb2520cd473#.9b5v7lrpp>. Accessed: Jan. 7, 2017.
- [18] M. Hachman, "The price of free: How apple, Facebook, Microsoft and Google sell you to advertisers," *PCWorld*, 2015. [Online]. Available: <http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html>. Accessed: Jan. 7, 2017.
- [19] B. Krebs, "Experian sold consumer data to ID theft service," in *KrebsonSecurity*, 2013. [Online]. Available: <http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/>. Accessed: Jan. 10, 2017.

[20] K. Jennings, "How your doctor and insurer will know your secrets — even if you never tell them," in *Business Insider*, Business Insider, 2014. [Online]. Available: <http://www.businessinsider.com/hospitals-and-health-insurers-using-data-brokers-2014-7>. Accessed: Jan. 13, 2017.

[21] "How Facebook makes money from personal data," in *Privacy Trust*, 2016. [Online]. Available: <https://www.privacytrust.com/blog/how-facebook-makes-money-from-personal-data.html>. Accessed: Jan. 13, 2017.

[22] C. Timberg, "For sale: Systems that can secretly track where cellphone users go around the globe," in *Washington Post*, Washington Post, 2014. [Online]. Available: https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html?utm_term=.cc89d34ef9fc. Accessed: Jan. 13, 2017.

[23] G. McFarlane, "How Facebook, Twitter, social media make money from you," Investopedia, 2014. [Online]. Available: <http://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx>. Accessed: Jan. 13, 2017.

[24] "States' Hospital Data for Sale Puts Patient Privacy in Jeopardy," in *Annual Medical Report*, 2013. [Online]. Available: <http://www.annualmedicalreport.com/states-hospital-data-for-sale-puts-patient-privacy-in-jeopardy/>. Accessed: Jan. 15, 2017.

[25] "Hospital Data: Verified Hospital Emails and Data Lists Available!," in *SK&A - QuintilesIMS*, 2017. [Online]. Available: <http://www.skainfo.com/databases/hospital-data>. Accessed: Jan. 15, 2017.

[26] "Consumer data broker ChoicePoint failed to protect consumers' personal data, left key electronic monitoring tool turned off for Four months," in *Federal Trade Commission*, 2009. [Online]. Available: <https://www.ftc.gov/news-events/press-releases/2009/10/consumer-data-broker-choicepoint-failed-protect-consumers>. Accessed: Jan. 10, 2017.

[27] B. Krebs, "Data broker giants hacked by ID theft service," in *KrebsonSecurity*, 2013. [Online]. Available: <https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/>. Accessed: Jan. 9, 2017.

[28] B. Krebs, "Data broker hackers also compromised NW3C," in *KrebsonSecurity*, 2013. [Online]. Available: <http://krebsonsecurity.com/2013/10/data-broker-hackers-also-compromised-nw3c/>. Accessed: Jan. 10, 2017.

[29] J. Apple, "FTC settles with data brokers in sale of consumer data used for illicit purposes," in *White & Case*, 2016. [Online]. Available: <http://www.whitecase.com/publications/article/ftc-settles-data-brokers-sale-consumer-data-used-illicit-purposes>. Accessed: Jan. 12, 2017.

[30] S. Thielman, "Experian hack exposes 15 million people's personal information," in *The Guardian*, The Guardian, 2015. [Online]. Available: <https://www.theguardian.com/business/2015/oct/01/experian-hack-t-mobile-credit-checks-personal-information>. Accessed: Jan. 10, 2017.

[31] P.-O. Dehay, "The (dis)information mercenaries now controlling trump's databases," Medium, 2017. [Online]. Available: <https://medium.com/@pdehay/the-dis-information-mercenaries-now-controlling-trumps-databases-4f6a20d4f3e7#.me4v5ijo7>. Accessed: Jan. 7, 2017.

[32] N. D. Goldstein and A. D. Sarwate, "Privacy, security, and the public health researcher in the era of electronic health record research," *Online Journal of Public Health Informatics*, vol. 8, no. 3, Dec. 2016. [Online]. Available: <http://www.ojphi.org/ojs/index.php/ojphi/article/view/7251>. Accessed: Jan. 11, 2017.

[33] D. C. Barth-Jones, "The 're-identification' of governor William Weld's medical information: A critical re-examination of health data identification risks and privacy protections, then and now" Jun. 2012. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397. Accessed: Jan. 11, 2017.

[34] L. Sweeny, "Matching Known Patients to Health Records in Washington State Data," Harvard University. Data Privacy Lab. White Paper 1089-1. June 2013. [Online]. Available: <http://dataprivacylab.org/projects/wa/1089-1.pdf>. Accessed: Jan. 11, 2017.

[35] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam, "I-Diversity: Privacy Beyond k-Anonymity," in *ICDE*, 2006. [Online]. Available: <http://www.cs.cornell.edu/%7Evmuthu/research/ldiversity.pdf>. Accessed: Jan. 11, 2017.

[36] B. Krebs, "Toward a breach Canary for data brokers," 2014. [Online]. Available: <http://krebsonsecurity.com/2014/12/toward-a-breach-canary-for-data-brokers/comment-page-1/>. Accessed: Jan. 12, 2017.

[37] T. Stafford, "How Liars Create the Illusion of Truth," in *BBC*, 2016. [Online]. Available: <http://www.bbc.com/future/story/20161026-how-liars-create-the-illusion-of-truth>. Accessed: Jan. 12, 2017.

[38] A. Chen, "The Agency," in *New York Times*, The New York Times, 2015. [Online]. Available: <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>. Accessed: Jan. 12, 2017.

[39] "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," in *Director of National Intelligence*, 2017. [Online]. Available: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Accessed: Jan. 10, 2017.

[40] J. Scott and D. Spaniel, *China's espionage dynasty: Economic death by a Thousand cuts* in *Amazon.com: Books*. CreateSpace Independent Publishing Platform, 2016. [Online]. Available: https://www.amazon.com/Chinas-Espionage-Dynasty-Economic-Thousand/dp/153532743X/ref=asap_bc?ie=UTF8. Accessed: Jan. 12, 2017.