Journal of Cybersecurity and Privacy

Tracked for Impact Factor

CITESCORE 5.3

Article

Use & Abuse of Personal Information, Part II: Robust Generation of Fake IDs for Privacy Experimentation

Jack Kolenbrander, Ethan Husmann, Christopher Henshaw, Elliott Rheault, Madison Boswell and Alan J. Michaels

Special Issue

Building Community of Good Practice in Cybersecurity

Edited by

Prof. Dr. Martin Gilje Jaatun, Dr. Hanan Hindy and Dr. Aunshul Rege

MDPI

https://doi.org/10.3390/jcp4030026

Journal of Cybersecurity and Privacy

MDPI

Article

Use & Abuse of Personal Information, Part II: Robust Generation of Fake IDs for Privacy Experimentation

Jack Kolenbrander, Ethan Husmann, Christopher Henshaw, Elliott Rheault, Madison Boswell and Alan J. Michaels *

Virginia Tech National Security Institute, Blacksburg, VA 24060, USA; jackkolenbrander@vt.edu (J.K.)
* Correspondence: ajm@vt.edu

Abstract: When personal information is shared across the Internet, we have limited confidence that the designated second party will safeguard it as we would prefer. Privacy policies offer insight into the best practices and intent of the organization, yet most are written so loosely that sharing with undefined third parties is to be anticipated. Tracking these sharing behaviors and identifying the source of unwanted content is exceedingly difficult when personal information is shared with multiple such second parties. This paper formulates a model for realistic fake identities, constructs a robust fake identity generator, and outlines management methods targeted towards online transactions (email, phone, text) that pass both cursory machine and human examination for use in personal privacy experimentation. This fake ID generator, combined with a custom account signup engine, are the core front-end components of our larger Use and Abuse of Personal Information system that performs one-time transactions that, similar to a cryptographic one-time pad, ensure that we can attribute the sharing back to the single one-time transaction and/or specific second party. The flexibility and richness of the fake IDs also serve as a foundational set of control variables for a wide range of social science research questions revolving around personal information. Collectively, these fake identity models address multiple inter-disciplinary areas of common interest and serve as a foundation for eliciting and quantifying personal information-sharing behaviors.

Keywords: fake identity; privacy; active OSINT; open source intelligence

Citation: Kolenbrander, J.; Husmann, E.; Henshaw, C.; Rheault, E.; Boswell, M.; Michaels, A.J. Use & Abuse of Personal Information, Part II: Robust Generation of Fake IDs for Privacy Experimentation. *J. Cybersecur. Priv.* **2024**, *4*, 546–571. https://doi.org/10.3390/jcp4030026

Academic Editors: Pierangelo Rosati, Hanan Hindy, Aunshul Rege and Martin Gilje Jaatun

Received: 29 May 2024
Revised: 5 August 2024
Accepted: 8 August 2024
Published: 11 August 2024

1. Introduction

The Use and Abuse (U&A) of Personal Information (PI) project [1,2] aims to capture and quantify how vulnerable PI is to sharing, uniquely attributing PI leakage to responsible parties as well as exploring whether certain identity characteristics, account patterns, or other online behaviors make us more vulnerable to sharing behaviors or other malicious activity [3]. Online users consistently share personal information with entities, hoping for security and anonymity. From online social networks to news and entertainment subscriptions, the vast majority of Americans are faced with the inherent trade between PI usage and resulting benefits in agreeing to customized online services. It is widely recognized that users' PI, as well as their online behaviors, are being tracked while web browsing. Previous studies identified more than 500 different tracking methods used by different sites, and certain pages have trackers that are connected to multiple parties [4]. Beyond this consensual sharing of our personal information [5], we inherently run the risk of data breaches [6,7], insider threats [8], corporate mergers or bankruptcies [9], or good old fashion misuse [10] leading to the release of our personal information. It is estimated that the average person has hundreds of possible threat vectors for the release of their personal information used in establishing those accounts.

Our broader research aims to develop a semi-automated open source intelligence (OSINT) system that allows for controlled sharing of falsified PI to be collected across SMS text, email, and voice domains [2]. To seed these tests of online PI sharing behaviors, we

require a robust automated method to generate realistic fake identities, expanding from a previous project's 300 manually created fake identities [1] to a flexible database of 1M (or more) fake identities. Additionally, we have found that this same infrastructure will support a wide range of quantitative social science experiments using the same fake ID methodology [11]. This paper highlights the methodology used to create and validate a scalable fake ID generator for these U&A experiments, which span a variety of topics from individual privacy to all kinds of quantitative social science questions.

1.1. Motivation

The motivation for this work is to create a custom model to efficiently generate fake identities as well as an underlying active OSINT collection system to support the large-scale deployment and data collection processes in order to understand how an individual's personal information propagates throughout the internet after signing up to second-party organizations. To effectively accomplish this, our work also aims to understand what information is necessary to create a reputable digital identity as well as how that information is processed. Additionally, this work aims to understand how an individual can create and utilize a fake account to remain pseudo-anonymous on the internet while simultaneously avoiding being removed by fake account detection algorithms. Further understanding of all of these items is necessary to allow individuals to protect their PI, while also being able to benefit from the digitalized world.

Users are often left in the dark without a thorough understanding of how their data are processed and utilized by companies and organizations [12]. Although companies implement privacy policies, they are typically confusing legal documents meant to protect the company itself rather than the individual [13,14]. To perform effective privacy research, researchers are often required to walk an ethical line to gain valuable insight and data. Typical research has long been guided by well-respected reports and documents such as the Belmont Report [15] and the Declaration of Helsinki [16]; however, the presence of big data is introducing new ethical questions that researchers must figure out how to approach [17]. Challenges such as the expectation of user privacy on digital systems, the effect of anonymization and de-identification of personal data on research quality, and the element of participant consent in big data research undertakings have led researchers to advocate for a revision and update of the typical guiding principles of research ethics [17–19]. The utilization of fake user accounts to perform privacy research allows researchers to circumvent and avoid many of the main concerns associated with big data privacy research [20]; to do so, researchers need the ability to generate and manage believable fake accounts at scale.

Similarly, to attempt to mitigate the spread of their PI, individuals often utilize impersonal or fake accounts to mask their identity on the Internet. Information that an individual marks as "private" on social media or digital sites can often still be accessed utilizing various OSINT analysis tools and processes [21]. This can subject individuals to privacy-related leaks or concerns, resulting in malicious activity involving their data and identity. In masking their information, non-malicious individuals want to be careful not to impersonate another individual or user. For these reasons, researchers and individuals alike are drawn to utilizing fake accounts, created using arbitrary personal information, on the Internet to mitigate the spread of their own private data [22–24].

Avoidance of Fake Account Detection

The main roadblock for individuals and researchers attempting to use fake accounts is the active effort by companies and organizations to remove them. Fake profiles and bots should be distinguished, as the first represents the public "face" and background of an online entity, while bots are the software element of a fake profile, which automates its activity in an effort to impersonate a human while online [25]. Malicious actors use fake accounts to carry out widespread attacks on social media and other platforms. These accounts can be utilized at scale to engage in phishing attacks or even shape public opinion online [26,27].

In 2022, Facebook reportedly removed 6.1 billion fake accounts from their platform, representing over two times their active monthly users [28]. These malicious accounts are often tied to spam, fake news, and other malicious campaigns. Malicious actors' utilization of fake accounts drives companies to implement robust account detection systems, impacting individuals' ability to maintain an active anonymous or pseudo-anonymous account for their own personal use. To generate and persist on the internet using fake accounts, individuals and researchers must often circumnavigate these malicious account detection algorithms, which requires knowledge of what features of a digital identity these algorithms use.

1.2. Ethical Considerations

Studies have been performed to help navigate the ethical considerations when applying fake personas for research purposes. Most of this work aims to protect stakeholders in online social networks. In such cases, the ethical considerations deal with protecting users, the providers of the service, and the advertisers and investors in such services. In terms of research, there are ethical ramifications regarding other users and their consent to be active in the study being conducted, and the indirect exposure of their information. Outside exposure of information, there is also the wasting of time or resources of other users or third parties invested in the network. An army of fake bots would actively be violating agreements required for the service, and waste server resources satisfying the requests of fake users. Further, depending on the influx of fake accounts, statistics that drive value and advertiser spending could be impacted [22]. Researchers in several cases have managed to infiltrate private organizations through strategic social bots targeting users involved in the organization [29]. Critics of this kind of information gathering have noted that a more ethical route would be designing a closed model to determine how vulnerable information might be taken or shared, but previous research has shown utilizing fake accounts in the real world is far more effective and can be conducted if certain limitations in size and scope are applied [30,31].

Using fake identities is a potent avenue of information gathering and enters into a challenging ethical arena when for most use cases of the technology effective data collection requires some level of deception. However, various international review boards have begun classifying risk levels to the implementation of fake identities for studies, especially in regard to OSNs. The three categories of research in this area are observational, interactive, and survey/interview [32]. Our use case falls under the *observational* research category, in that identities are being utilized as an instrument to safely observe how different entities interact with users and leverage their PI. Using real information to conduct such a study would be unethical according to several ethical guidelines that warn against placing compromising information at risk. We have, therefore, bounded our fake IDs by intentionally limiting the scope of information used in creating them (e.g., no social security numbers, driver's license numbers, etc.), and actively de-validating any data that could be traced back to a real source, such as our random address generation. In addition, though the project aims to generate 100 K IDs, only a small number of IDs are dedicated to fake accounts at any one service provider, minimizing the impact on the hosts. Should other experiments or operations legally require fake identities that possess such information, the assignment of the additional information can follow similar models as described previously. Additional evaluations of the ethical considerations for active OSINT research, including a self-evaluation of the Use and Abuse project against criteria provided in the Department of Homeland Security's *Ethics and OSINT Scorecard*[33] is provided in [11].

1.3. Paper Outline

Given this foundation of research activity leveraging fake identities for a variety of research topics, this paper seeks to demonstrate a scalable and realistic fake identity generator that can reasonably withstand human and machine inspection for many candidate research problems. A brief overview of the ongoing efforts and current Use and Abuse

of Personal Information system architecture [11] is provided in Section 2. To effectively employ fake accounts for privacy research, as well as to create a robust fake account generator, it is necessary to understand what characteristics compose a digital identity. A model for understanding the components of an effective digital identity is developed through a comprehensive literature review in Section 3. The design and development of the process for the controlled formulation of the fake identities from a pseudorandom source is described in Section 4, focusing on ensuring that IDs are complete and ethically sourced. A brief look at fake identity generation extensions and discussion surrounding the adaptation of the fake identities to specific privacy or social science experiments is then provided in Section 5. A more in-depth overview of the employment of fake identities for privacy research as well as the collection architecture is provided in a separate paper [11]. Finally, a series of conclusions and next steps are provided in Section 6. The contributions of this paper are threefold: a model is formulated for the composing characteristics of reputable digital identities through a detailed literature review, an easily repeatable and adaptive process for the creation of tailored fake digital identities for privacy research is created using a Pseudo Random Number Generator (PRNG), and a series of extensions is provided to further strengthen the digital identities and accomplish the objectives of the Use and Abuse Project.

2. Use and Abuse of Personal Information Project

The use of fake identities, and more generally fake online accounts, is common for privacy research [34,35] and a variety of malicious use cases [36]. The Use and Abuse of Personal Information project is an ongoing research effort to create a system capable of supporting large-scale active open-source intelligence (OSINT) research using fake PI to answer privacy and quantitative social science questions, as described more extensively in a companion paper [11]. A previous iteration [2] of the Use and Abuse research project yielded valuable information for what PI is required to establish accounts, creating a foundation for experimentation at scale. The overarching goal of the Use and Abuse research is to answer research questions such as:

- How does our personal information propagate and spread on the internet after signing up to second-party organizations?
- Is it possible to predict the election winners based on an analysis of the amount and content of communications received from the candidates?
- Do airlines and travel companies target and market towards certain income or personal demographics differently?
- Do health and supplement companies target certain age or gender demographics differently than others?
- Is a certain gender, race, or ethnicity more likely to receive communications from a company after uploading their resume to a job board?

These are just a few examples of potential research questions that could be answered using the communications collected from surrogate PI. For each question, a subset of fake IDs can be created, and signed up to the targeted organization or group, and then the communications and content received can be analyzed.

3. Literature Review

Fake accounts and identities have been researched and utilized for many different types of malicious and non-malicious applications. Fake profiles and bots are common amongst both online scammers and large government entities. Phishing attacks, using a combination of accounts embedded in online social networks and social engineering techniques, have been on the rise with a 2015 Verizon study showing of 150 K phishing emails, 23% were opened by the target, with 11% of total recipients opening attachments in those emails [37]. Phishing with these accounts has only become more prevalent across online social networks as fake profiles and automation techniques continue to advance.

Foreign governments invest in fake accounts and bot techniques with the intention of shaping public opinion or sowing discord amongst targeted political groups [38]. In 2019, studies evaluated how the state-sponsored Russian Internet Research Agency posted more than 1.8 M images to Twitter from a variety of accounts they managed. The study showed that the activity of the accounts coincided with political rallies both in terms of the timing of account activity as well as the political message expressed in the images being shared. Accounts targeted both sides of the political spectrum in the US to intensify and polarize opposing political viewpoints [39]. Even more recently, fake account activity has been tied to impacting public sentiment regarding the COVID-19 pandemic [40]. In summary, within a research context, fake accounts or identities are generally applied to determine the risks of group infiltration impacting public sentiment in an online forum. Using fake accounts themselves as the mechanism for determining how information is shared as a form of active OSINT collection, such as described in this paper, is far less common.

Although there has not been a large body of work employing fake identities for privacy research, work has been conducted to determine the extent, process, legality, and potential solutions to the sharing of personal information on the Internet. The understanding of personal privacy on the Internet is a complex, multifaceted issue that has real-world implications for a variety of individuals, groups, and law enforcement agencies [41]. As OSINT requires data to be publicly available online, companies and researchers have developed cryptographic algorithms and protocols to mitigate public data exposure [42]. Employee PII exposure represents a key vulnerability for companies and employees alike, leaving them vulnerable to phishing and social engineering attacks. This has led companies to seek methods to mitigate the risks associated with public employee PII and data on social media and other platforms [43].

In addition to mitigating exposure of PII information, other tools have been created to detect PII collection and transmission. One example is the implementation of AI to detect PII in images [44]. Another tool, PIITracker, uses reverse engineering techniques to track and determine if a program or process collects and transmits PII data [45]. Similarly, solutions implementing data loss prevention (DLP) principles have been designed and developed to detect PII breaches on company systems [46]. There has also been a variety of investigative works focusing on understanding how PII data are leaked in various online use cases, including web cookies, mobile networks, and online social networks [47–49]. Understanding how third-party data brokers utilize PII data to carry out targeted advertising is another domain that is being researched to determine the associated privacy risks and impact on individuals [50,51]. Although beneficial to enhancing individuals' understanding of their privacy online, these works typically focus on one domain or section of user privacy, rather than attempting to develop a full picture. While using the Internet, an individual utilizes many different applications, and therefore, has a variety of potential PII leaks and risks. As a result, a wider understanding of individual privacy is necessary.

In privacy research using fake accounts, the vast majority of research has demonstrated interest in determining the impact fake account activity has on other users, and how they might be detected. However, a few research teams have utilized fake accounts themselves as the mechanism used to gather data and study online interactions [52,53]. In 2011, research was conducted using both passive and active fake accounts or "socialbots" orchestrated together to demonstrate the vulnerability of PI [54]; methods to identify fake accounts have improved significantly since then, using techniques like correlating activity across IPs and geographic locations, increasing the threshold for constructing a *good* fake ID. There are a variety of open-source platforms that provide automated mass account generation functionalities for different websites and social media platforms [55]. These platforms, however, do not allow for private, localized account generations or the level of customization needed for the Use and Abuse Research project.

Previous research in this area shows that utilizing fake accounts can be an extremely effective way to collect meaningful data, and any automated fake accounts must be robust enough to avoid continually improving detection techniques [22,56]. To successfully

create fake accounts that are capable of persisting and avoiding detection algorithms, it is necessary to understand what features and techniques the implemented algorithms utilize. There is a large amount of literature and work conducted on the creation and implementation of these algorithms, thus delving into this body of research allows for the determination of the characteristics that contribute to a robust and legitimate account. The discovery of fake accounts or the ability to correlate all of them due to a related pattern on a single social network could compromise the surrogate accounts, impacting experimentation and the collection of data, emphasizing the need for believably robust identities for privacy research.

3.1. Determining Information Required to Create a Fake Account

Efforts have been made to map what primary behaviors and qualities establish online profiles and identities. These include presence, relationships, reputation, groups and identity [57]. This also includes direct conversations and active sharing directly between different users [58], which suggests the need for automated interaction from the fake identity's account. A convincing online profile should engage in these behaviors actively to anchor itself convincingly in the world and avoid detection. Researchers can form a model to generate *good* fake identities for privacy research purposes by researching and determining what features are most commonly analyzed for detection.

Research surveying different machine learning (ML) algorithms has been able to identify fake accounts with up to 98% accuracy in certain cases [59], based primarily on behavior patterns and characteristics. Studies conducted analyzing accounts on Twitter utilized a combination of methods when identifying bots and their fake accounts. A multi-pronged approach with a machine learning model using account activity, information, and metadata as inputs allows for a more effective fake account detection [60]. An analysis of the variety of implemented detection methods can enable researchers to ascertain the defining characteristics of an effective fake identity.

Through a comprehensive review of privacy and fake account detection literature trends and characteristics can be identified, and therefore, focused on when designing a fake account generation model. Additionally, conclusions can be made about which characteristics are necessary for effective accounts within different internet applications. Identities employed in some domains, such as social media applications, will require additional fake characteristics when compared to an identity used for newsletters or blogs. To remain plausible, a social media identity may require fake posts, interactions, comments, etc. Table 1 identifies a variety of internet applications, examples of organizations or companies that fall under that category, as well as their defining features regarding privacy research identities. Although not exhaustive, the various internet applications represent the sliding scale of how much information is required to generate an account for that purpose.

The content in Table 1 provides eight generalized categories of different internet applications. The applications are divided based on the content required for an individual to generate an account on that type of platform. The category column provided a high-level overview of the characteristics of accounts that fall into that section. The example items column provides specific examples of groups or websites that fall into that category while the notes column provides a more in-depth explanation for those items. Finally, the acronym column maps the category to a short-hand acronym that is utilized to map account characteristics to websites in Table 2. The categories range from investment brokerage and gambling websites, which require a user to provide identification documents and social security numbers, to websites that do not require a user to provide any information to access content. Intermediate categories include websites that solely require a user to provide basic information to gain access to a service or content, websites that require a one-time or saved payment method, streaming platforms, and social media websites. Overall, Table 1 provides a generalized overview of various internet applications categorized by the breadth of information a user is required to provide to generate an account for that purpose.

Table 1. Internet Applications and Their Defining Characteristics Required for Account Creation.

	Website Category	Example Items	Notes	Acronym
1	Identification Required	Investment Brokerages, Banks, Gambling Websites, Insurance Brokers	Websites or organizations that require an individual to provide identification numbers such as social security or tax identification numbers and/or websites that require an individual to upload a driver's license or passport documents.	ID
2	Social Media	Instagram, Facebook, Twitter, Snapchat, etc.	Social media websites that require an individual to create an account to engage in sharing and interaction of content on the platform.	SM
3	Streaming	Netflix, Hulu, HBO, YoutubeTV, Peacock, etc.	Websites and companies that require an individual to pay a fee regularly to engage with and watch content on the platform.	SW
4	Online Shopping	Amazon, eBay, Home Depot, Nordstrom, H&M, etc.	Websites that allow users to purchase goods and services but require an individual to provide a shipping destination and payment method.	OS
5	Paywall	New York Times, Wall Street Journal, The Washington Post, etc.	Websites that allow a user to view content after making an account and providing a payment method.	PW
6	Blogs and Chat Boards	Reddit, Discord, Quora	Websites that allow many individuals to engage with each other and browse/share content	BL
7	Email and Online Communication	Gmail, Outlook, etc.	Websites that allow a user to create and utilize an e-mail platform to communicate with individuals and groups.	E
8	Free Access	Wikipedia, Encyclopedia, News Websites, etc.	Websites that allow users to read and see content and information without the requirement of creating an account to do so.	FA

Table 2. Digital identity characteristics (categories in gray blocks) and their required usage across various accounts on the internet. The internet application categories, from left to right, are News Websites and Wikipedias, E-mail and Online Communications, Blogs and Chat Boards, Paywall Websites, Online Shopping Platforms, Streaming and Content websites, Social Media Websites, and Investment, Gambling, or Insurance websites. A full circle symbolizes that the characteristic is always required or mandatory for creating an account within that domain. A partially filled circle indicates that the characteristic is sometimes required or an optional input field. Finally, an empty circle represents that the characteristic is seldom used to create an account within that domain.

	Internet Applications								
Characteristic	**FA**	**E**	**BL**	**PW**	**OS**	**SW**	**SM**	**ID**	**Relevant Citations**
Sensitive PII									
Education	○	○	○	○	○	○	◐	●	[61,62]
Email Address	○	●	●	●	●	●	●	●	[23,63–65]
Employer	○	○	○	○	○	○	◐	●	[61,66,67]
Gender	○	○	○	○	◐	○	●	●	[23,62,68–70]
Name	○	●	●	●	●	●	●	●	[61,67,71–73]

Table 2. *Cont.*

	Internet Applications								
Characteristic	**FA**	**E**	**BL**	**PW**	**OS**	**SW**	**SM**	**ID**	**Relevant Citations**
Confidential PII									
Address	○	○	○	●	●	●	○	●	[64,65,74]
Age	○	◐	◐	○	◐	●	●	●	[68,75]
Birthdate	○	●	●	◐	◐	●	●	●	[65,66,74,76]
Geographic Location	○	○	○	◐	◐	◐	●	●	[68,72,77–79]
IP Address	○	○	○	○	○	◐	●	●	[61,80,81]
Phone Number	○	◐	○	●	●	●	●	●	[66,73,81–83]
Relationship Status	○	○	○	○	○	○	◐	●	[23,62,66]
Religion	○	○	○	○	○	○	◐	○	[23,69]
SMS Number	○	◐	○	◐	◐	●	●	●	[84,85]
Username	○	●	●	●	●	●	●	●	[56,67,73,78,86]
High-Risk PII									
Drivers License or Passport	○	○	○	○	○	○	○	●	[74]
Facial Recognition	○	○	○	○	○	○	◐	●	[61,75]
Medical Records	○	○	○	○	○	○	○	◐	[69]
One Time Payment Information	○	○	○	●	●	●	◐	○	[87–89]
Password	○	●	●	●	●	●	●	●	[90,91]
Saved Payment Information	○	○	○	●	○	●	◐	●	[87–89]
Social Security Number	○	○	○	○	○	○	○	●	[74,92]
Digital Behaviors and Identity									
Activity Time	○	○	○	○	○	○	●	○	[80]
Accounts Followed	○	○	◐	○	○	○	●	○	[71,78–80,86]
Comments	○	○	◐	○	○	○	●	○	[76,80,93,94]
Followers	○	○	◐	○	○	○	●	○	[71,77,80,93,95]
Friendships	○	○	◐	○	○	○	●	○	[67,71,77,93,96]
Hashtags/Threads	○	○	◐	○	○	○	●	○	[86,96,97]
Likes/Favorites	○	○	◐	○	○	○	●	○	[56,70,94,95,98]
Posts	○	○	◐	○	○	○	●	○	[70,72,79,93,94,96]
Profile Banner	○	○	○	○	○	○	●	○	[77,78,95]
Profile Description	○	○	◐	○	○	○	●	○	[98–101]
Profile Image	○	◐	◐	○	○	○	●	○	[68,99–102]
Tags/Mentions	○	○	○	○	○	○	●	○	[79,86,96,97]
Digital Metadata									
Account Age	○	○	○	○	○	○	●	○	[56,97]
Increase in Friendships/Connections	○	○	◐	○	○	○	●	○	[63,95,103]
Time of Account Creation	○	○	○	○	○	○	●	○	[61,68,98,101,102]
Timing of Posts	○	○	○	○	○	○	●	○	[76,102]
URLs Present in Profile	○	○	○	○	○	○	●	○	[99,100]

Table 2 provides a mapping of various characteristics that compose an online profile for an individual to the various internet applications that require that characteristic. The characteristic column consists of all account characteristics that were present in the privacy and fake account detection works reviewed in the literature survey. Characteristics range from non-digital identifying information such as name, birth date, and social security number to digital identifying information such as username, email, and phone number. Traditional PII is often split into three categories: Sensitive, High-Risk, and Confidential [104]. Sensitive PII refers to publicly available information that can be found online or through social media, such as name and gender. Confidential PII refers to information that can often be found through extensive research, however, individuals would typically prefer to remain private. Finally, high-risk PII refers to information that can result in identity theft or result in real damage to an individual if accessed, such as SSN and credit card information [104]. Some digital information does not fall into one of the traditional PII categories but can be used to construct an identity or gather information about an individual. As a result,

digital behaviors and identities as well as digital metadata categories are considered in this paper to be legitimate components of a digital identity. Within the table, characteristics are divided into five different categories: Sensitive PII, Confidential PII, High-Risk PII, Digital Behaviors and Identity, and Digital Metadata. A fully solid circle indicates that the corresponding trait is generally required to create an effective, believable account on a website in that category. A partially filled circle means that the characteristic is occasionally or sometimes required for websites in that category. Finally, an empty circle indicates the characteristic is seldom or never used in an account creation. The categories of websites are not exhaustive, however, they provide an overview of the range of account types that exist when using the Internet.

Using the information in Table 2, requirements can be created for which characteristics are required to create a fake identity for that internet purpose. Each detection process employs a different underlying algorithm yet utilizes similar input data. To perform effective privacy on social media and streaming sites requires more information than blogs and communication sites. Social media research and accounts require further human-like interaction such as the posting of content, interaction with content, and scrolling. As a baseline, most websites require an e-mail address, username, and password. Social media represents the most involved domain that researchers can legally employ fake IDs in to answer research questions. Overall, the content in Table 2 allows a researcher to create a well-rounded overview of digital identity characteristics that are required to create *good* fake identities for privacy research.

3.2. Example of a Fake ID

This paper considers the construction of fake IDs such that they can pass automated inspection techniques (if any) and thus be well suited to privacy or social science experimentation. As such, the richness of the identity must be sufficient that we can easily answer personal questions on behalf of the fake person, such as an example, Bella Tessier, highlighted in Figure 1 (you can call and email Bella, although you may reach her voicemail and need to wait for the Use and Abuse Account Interaction Engine to take her turn for responding). Moreover, the personal characteristics should adhere sufficiently to population demographics so that privacy experiments are not biased by ID selection (unless, of course, identity characteristics are in fact the subject of the experiment). Notably absent from her dossier are federally controlled identifiers like a Social Security number or others that could lead to illegal activity. While the Use and Abuse research project [11] is much broader, this paper performs a deep dive on the generation of fake identities and their characteristics, which may be applicable to other forms of privacy research.

Figure 1. An example of default characteristics for a single fake identity, Bella Tessier . The front of the identification card provides a visual representation of the personal identification characteristics that would be found on a typical identification card. The rear of the identification card provides further characteristics of identity, such as gender, race, employment, security questions, education, etc.

4. Constructing Realistic Fake Identities

Each identity must be unique, internally consistent, and defined well enough to be useful across different research interests. Uniqueness allows for the identities to stand up to basic human scrutiny and allows researchers to test how different demographic characteristics affect PI usage or sharing behaviors. This allows for a deeper analysis of what information is most valuable as well as an understanding of the motivations of the entities using it. In addition to answering questions about the level of privacy a general person can expect online, unique identities spread across demographics allow researchers to analyze differential behaviors across demographics. The same level of depth is applied to all the identities (excluding highly specialized cases), even if the content may not be used so that the process of identity assignment can be automated efficiently. This way, researchers can take large batches of identities and assign them all at once with a high level of confidence that the generated backgrounds of the individuals will serve the needs of their use case. As the identities are constructed with random and unique characteristics, as shown in Figure 2, this process must be managed such that no conflicting attributes are assigned to the same fake person. For example, the birthday and age of a person must be internally consistent, and it would be reasonable to assume certain first or last names of individuals should align with their background, ethnicity, and gender. All of these considerations must work in concert to generate identities that stand up to cursory human or automated scrutiny, preventing detection of the fake identity and thus improving the reliability of the project's conclusions.

The generation of realistic IDs that withstand reasonable scrutiny relies on mapping outputs from a pseudorandom number generator (PRNG) source [105–107] discussed in Section 4.4, previously shown to approach maximal entropy to a range of attributes in rough proportion to their relative occurrence within the US population. Alternative PRNG-based approaches may be used, though most PRNGs do not permit a look-ahead state translation that is assumed here, enabling semi-independent and repeatable generation of fake IDs from a base seed. Each resulting ID is engineered to be unique to simplify subsequent data analysis and internally consistent to reduce the probability of errors during signup. Baseline IDs feature attributes previously commonly solicited during signup events [2] as well as expandable, not-yet-defined attributes that may be tailored to subsequent experimental questions.

As generated, each unique fake ID consists of a .bin entry comprising a series of 256 16-bit PRNG output values; 256 attributes (easily expandable) were deemed sufficient to encapsulate all the feasible characteristics of a fake identity and pass modest scrutiny and address most research questions, while 16-bit outputs from the PRNG permit the selection of up to (2^{16}) potential values for each of the attributes, granting us a large range of possible values for attributes with high variability. For attributes with a continuous or extremely high distribution of values, such as frequency-weighted names, 32-bit PRNG output values were achieved by concatenating two sequential 16-bit PRNG output values and mapping the attribute to the two adjacent fields rather than just one; a small loss of entropy can occur [107] if the ratio of PRNG states and distribution frequencies are not well considered. Finally, capping the IDs at 4 Kbit (512 bytes) reduces the storage burden for large experiments, though subsequent outputs from the PRNG could be used to scale the number of attributes or attribute values in response to future experimental needs.

Once the fake ID .bin entries were generated, we defined iterated attributes #1-256 in a lookup table. The next step was to map attribute values in accordance with their relative frequency in the US population. Demographic frequencies were sourced from a variety of sources, including the US census. Itemization of the foundational ID attributes is displayed in Table 3.

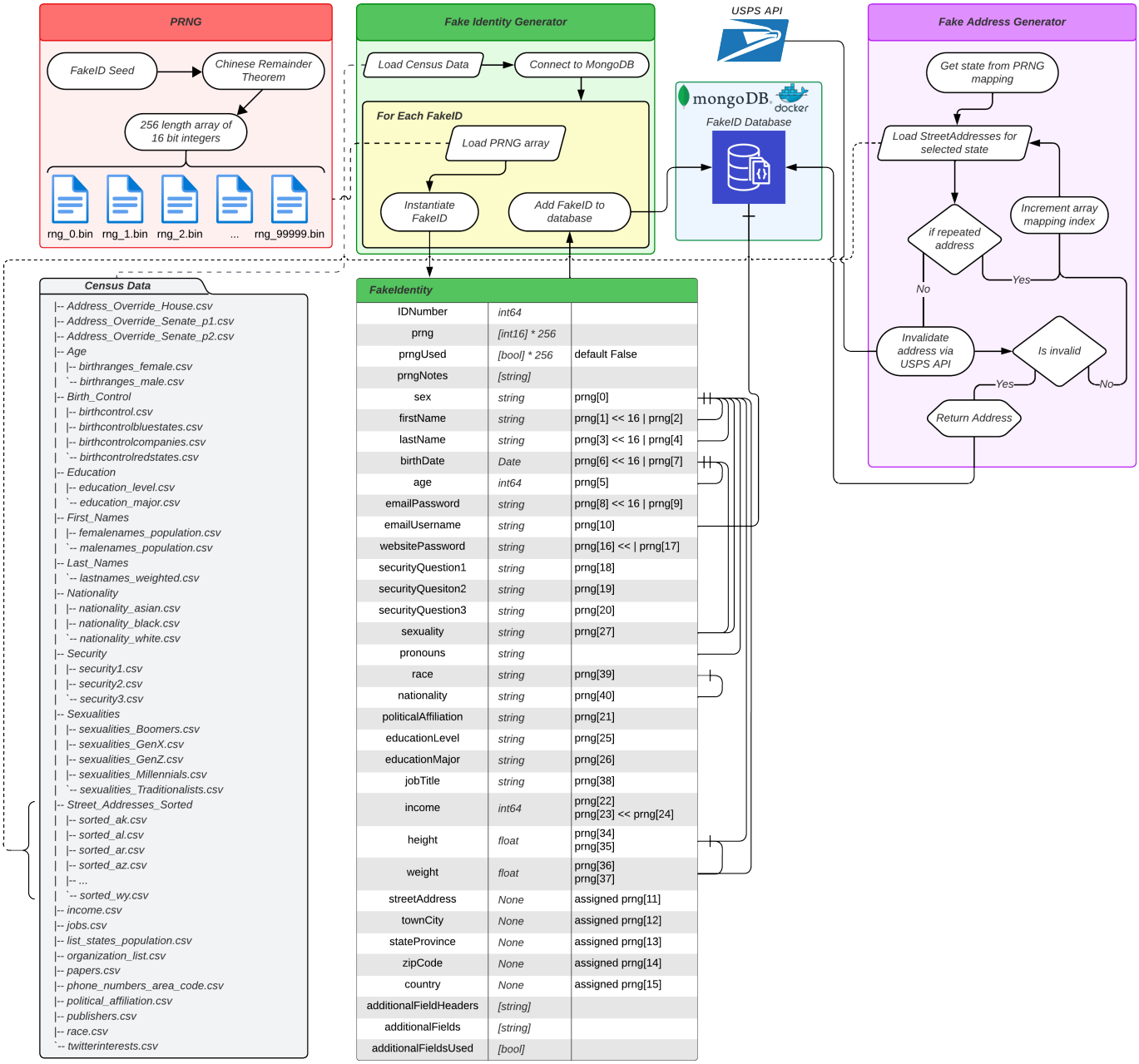

Figure 2. Top-level process for generation of fake IDs.

For identity characteristics that are mapped according to discrete distributions, the overall selection process is based on either weighted (e.g., race or gender) or percentile-based (e.g., income) mappings. These frequencies were then used to generate weighted attribute value lists by replicating common entries a number of times equivalent to the value divided by the Greatest Common Divisor (GCD) of all attribute values. These weighted lists were then mapped to masked, modulo-reduced PRNG output values, resulting in a distribution of attribute values that tracks US population frequency distributions. Care was taken to prevent internal inconsistencies by focusing on fundamental characteristics (e.g., birthdate) and then calculating secondary characteristics (e.g., age) or considering conditional distributions (e.g., height and weight) that conform. As a result, a number of logical adjustments or constraints were made to the mapping process.

Table 3. Mapping of PRNG word outputs to foundational fake ID characteristics.

PRNG Output	ID Characteristic	Distribution Shaping	Rationale
0	Sex and Preferred Pronoun	Male: 50%, Female 50% Pronouns assigned to sex	2010 Census [108]
1–2	First Name	Weighted 15 k (male) and 20 k (female) most common names	Social Security Administration [109]
3–4	Last Name	Weighted 20 k most common surnames	2010 Census [110]
5–7	Birthdate	Adult Ages (18–74), 5-Year Bracketed Frequencies by Sex	Census [111]
8–9	Email Password	Unique per ID	
10	Email Username	Unique per ID	
11–17	Address (split into 5 columns)	Unweighted, Pseudo-random Street Assignment based on Geographical Frequency by State, Invalided by the USPS API	2020 Census [112] Open Address [113] USPS [114]
18	Security Response 1	Uniformly Assigned List of Popular Movies	
19	Security Response 2	Uniformly Assigned List of Cities	
20	Security Response 3	Uniformly Assigned List of Colors	
21	Political Affiliation	Democratic 51%, Republican 47%, Third-Party 2%	2020 election [115]
22–24	Income	\$15 k–\$25 k : 10%, \$25 k–\$35 k: 11%, \$35 k–\$50 k: 14%, \$50 k–\$75 k: 20%, \$75 k–\$100 k: 15%, \$100 k–\$150 k: 20%, \$150 k–\$200 k: 10%	Statistica [116]
25	Education Level	Weighted Educational Attainment Brackets	Census Bureau [117]
26	Education Major	Weighted Educational Major Brackets	Statistica [118]
27	Sexuality	Sexual Orientation and Identity by Generation	Gallup [119]
28	Salutation	Associated by Sex	
29–33	Reserved		
34–35	Height	Gaussian with U.S. mean $\pm 2\sigma$	CDC 2015-2018 [120]
36–37	Weight	Gaussian with U.S. mean $\pm 2\sigma$	CDC 2015-2018 [120]
38	Job Title	Weighted National Employment Matrix	U.S. Bureau of Labor Statistics 2021 [121]
39	Race	White 75.80%, Black 13.60%, Asian 6.10%, Other 4.50%	U.S. Census Bureau Population Estimates [122]
40	Nationality White	Hispanic 18.90%, Non-Hispanic 81.10%	U.S. Census Bureau Population Estimates [122]
40	Nationality Black	Hispanic 2%, Non-Hispanic 98%	Pew Research [123]
40	Nationality Asian	Hispanic 0.002%, Non-Hispanic 99.998%	Pew Research [124]
41	Website	Assigned based on Research Question	
42–255	Reserved		

4.1. Derived Fields

- **First Name**: separate first name lists based on U.S. Census data were used for each of the male and female IDs. A larger list of female names was used than male names given what appears to be higher variability (particularly in spellings) in female names.

- **Sex**: these values were assigned 50/50 instead of 49.2 and 50.8; for any experiments where those distinctions are relevant, we anticipate more extreme sculpting of gender identities.
- **Birthday/Age**: the PRNG-based mapping creates a birthdate, while age is directly calculated with the current date at any usage of age.
- **Address/State**: state was selected first and an address was generated for that state.
- **Address**: uses the USPS API (usps-api 0.5) [114] to determine if a generated address is fake or not. Returns true or false, with all street numbers modified until the result is confirmed as false.
- **Height/Weight**: once Height has been selected from a percentile-based distribution [120], a conditional distribution was used to select a corresponding weight that is within two standard deviations of the height-adjusted median.
- **Ethnicity/Nationality**: these values used conditional distributions of the Hispanic ethnicity into the six racial categories employed by the US Census.
- **Education Level/Education Major**: Education Level was generated first and then if the education level was higher than a high school education, a major was assigned.
- **Salutation**: these values were originally mapped directly for salutations for males and females. Marriage and degree were not factored into these, but allow for distinctions for "Dr." or between "Ms." and "Mrs." if needed for individual questions.

Lastly, certain attributes were scrutinized for matching legitimate attribute values (e.g., address) to prevent the potential for fraud and spamming of unsuspecting individuals who happen to match our fake IDs. These adjustments are detailed below:

- **Phone**: we used only phone lines purchased and managed on FreePBX Trunking.
- **Address**: We invalidated addresses by USPS API, "re-rolling" the PRNG output in a controlled fashion to generate a new street address when an address number was returned as legitimate.

4.2. Tailoring Fake IDs to Meet Research Needs

For each of the fake IDs, these foundational attributes were determined to suit the needs of the vast majority of research questions. However, we also recognize that specific questions may require particular attributes outside our ability to pre-provision. In the case where a particular question requires attribute(s) not already generated, the next unused PRNG output is allocated to a custom mapping unique to that research question. This required us to find the data in association with the attribute and then map that value using a process similar to that above. Given that nearly 80% of the PRNG values are unallocated, the extensibility of base identities to much even richer frauds is up to the user. To maintain robustness, the process of adding new identity characteristics starts with finding a reliable distribution of the identified characteristic and then mapping based on discrete lookups, weighted lookups, distribution fits, or direct calculations. One of the key benefits of using this model where a "key" space is pre-allocated to identities in finite blocks is that the entire set of fake identities can be re-constructed from a blank initialization of the overall system. Various data formats were used in this overall mapping format, with binary files favored for the initial PRNG outputs and Mongo DB employed for managing the selected fake identities as distinct records.

4.3. Scope of Fake Identities

Careful distinctions must be made in considering what characteristics can be applied to an identity that provides a level of depth sufficient to answer meaningful research questions [1], while avoiding fraud or identity theft that might occur accidentally when generating IDs at scale. This requires that any information that could potentially tie back to a real person be validated as fake. In addition, no fake phone numbers will be used; we established our own phone server with 6000 live VoIP phone lines to receive/make calls and voicemails as well as send/receive text messages via custom FreePBX servers as one

additional avenue of data collection for the project. For our purposes, we have also decided that no true facial images will be used in account creation.

One of the most prominent challenges in limiting the scope of identities is in the invalidation of addresses. We initially define a population-weighted distribution of counties across the United States, acquiring valid zip codes and streets from those locations. We then randomly assign an invalid home or apartment number on a street. The realism of the address down to the specific street, as highlighted in Figure 3, permits internal consistency as well as passes cursory verification methods. Depending on the level of third-party address verification used by private companies [125,126], the real region could pass as valid even though the particular house or apartment cannot be identified in a database of known addresses. Anecdotal evidence from our local Post Office suggests that any mail delivery person will have the addresses on their regular route fully memorized and likely discard or flag mail addressed to a fake address.

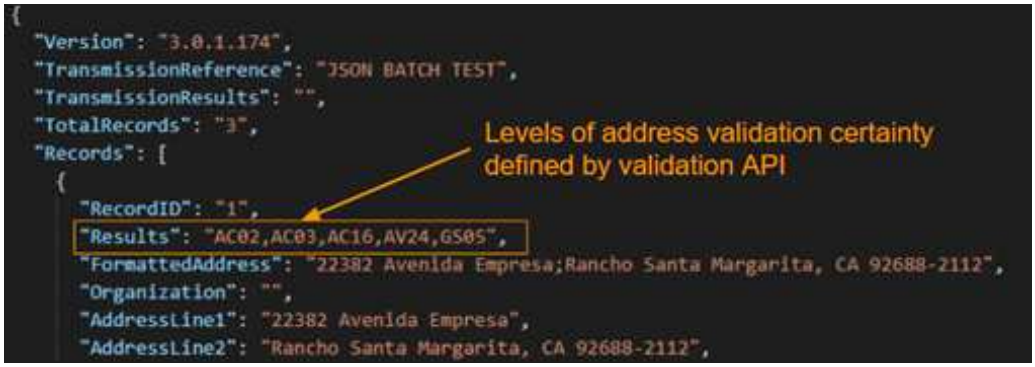

Figure 3. An image of address validation API with different levels of validation shown.

We leverage a similar technology as most private companies to incorporate address invalidation into the ID generation process, only with the reverse intent. When a house number is generated, an address lookup API verifies to a high degree that the address does not exist and is able to be applied to the fake person. If the address is valid, a new random house number is generated and the check is applied again. This process is repeated until an invalid address is created and applied successfully.

4.4. Pseudo Random Number Generation (PRNG)

The pseudo-random number generation is the first step in the ID generation process. The motivating factors for controlled PRNG as opposed to simply randomly generating and assigning numbers to each individual lies in its repeatability and flexibility for the U&A use case. We use a script derived from the residue number system (RNS)-based PRNG [105,106] that takes a base 320-bit base key and a set list of prime numbers to generate indexed sequences (length $\gg 10^{100}$) of 32-bit integers. The arbitrary seed value and RNS methods permit efficient parallelization of the PRNG process. RNS-based arithmetic is widely used for cryptography and simulation-based PRNGs [127,128] as well as similar commercial security applications [129,130].

Of particular value for the chosen PRNG is that if the database of identities were ever corrupted, the fake ID generation script can be simply run again with the same base seed, and all the same derived fake ID characteristics will be replicated. Should the data that are being aggregated together to create the fake IDs ever be breached, this also adds a barrier to creating an effective algorithm to reverse engineer the output stream [107]. Finally, this also ensures that a completely different set of pseudorandomly generated fake identities can be generated by changing the base key.

4.5. Fake ID Example

Each ID is organized in a non-relational MongoDB database with each JSON document, similar to that shown in Figure 4, representing one full identity, 100K of which are contained

within a single collection. Attributes highlighted in green are the pieces of information most services will require or allow a person to share. The attributes highlighted in yellow are used for internal management and identification of the IDs within the database. The unique ID is simply the sequential identifier assigned to each identity as it is created so that each person can be indexed, and all data collected for each person can be identified and related across different areas of the project. The "Rand Array" contains all random values generated by the PRNG, which were used to generate the identity and contains all the future values available for future attribute assignments. In total, 4096 bits of PRNG output are allocated to each fake ID.

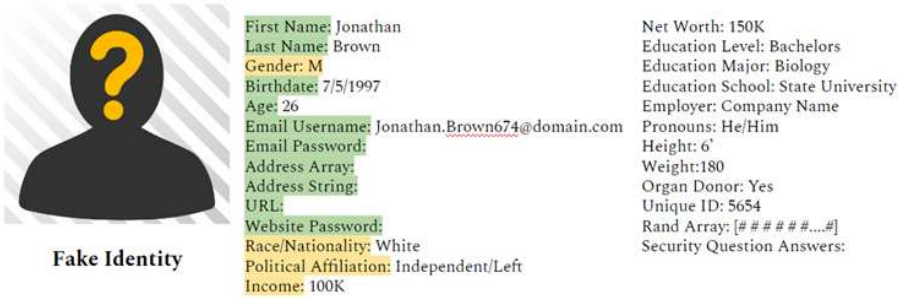

Figure 4. Image of an example ID with its attributes listed. All of the attributes listed are default for all IDs. If an ID needs an additional attribute, the title is placed in the additionalFieldHeaders section and the associated value is placed in the additionalFields section. If an attribute was used for the signup, then the corresponding index number will be set to True in the prngUsed section. If an attribute needs to be changed in any manner for the signup, then the prngNotes will reflect all changes made by listing the attribute and the value it was changed to for all applicable attributes. Additionally, the dateUsed and researchQuestion attributes are set upon signup completion.

Each ID must maintain a degree of internal consistency. For example, height and weight were tied together in the ID creation process in order to represent realistic physical attributes drawn from Gaussian ($\pm 2\sigma$) distributions mapped to averages in the United States. The raw data that are collected and then aggregated together to create the identities were collected from a variety of publicly available sources. Names, addresses, and possible occupations were all sourced from Social Security Administration [131] and US Census reports [132]. Height and weight data were informed by reports from the CDC [133]. Data regarding household income, and political affiliation were taken from a private research institution, the Statista Research Department [116,134]. In some cases, more PRNG bits are used than might appear minimally required, yet that is to help refine the fidelity of specific fields to appear more realistic (e.g., an income of $15,032 as opposed to choosing midpoints of the bottom income range of $20,000). These sources were utilized to provide the data themselves as well as the distribution of those data across different demographics. This allows the identities to be an effective and accurate emulation of real individuals as well as a model for studying online interaction at the macro scale, understanding the interactions of thousands of people who represent a broad and accurate distribution of *average* Americans. The primary goals of the project are met by individual identities and their interactions; however, in using distributions, the data are extensible to broader and more holistic research questions.

4.6. Raw Data Distribution

For most attributes, including the more generic first and last name attribute fields, each possible option in the raw dataset has a specific distribution within the dataset associated with it. This allows for the entire fake identities database to have a distribution of attributes tailored to reflect the backgrounds of US citizens more accurately, as well as offer the ability to set specific attributes of interests to have a higher likelihood of being represented among the fake IDs, without compromising the randomness of the ID generation process.

This distribution system was applied to more accurately generate individuals with unique backgrounds. Early iterations of the project used the top few thousand most common values for each attribute from previous census data but may have resulted in a lack of representation of minority groups. Adding a distribution to each individual identity characteristic slows down the initial setup of the raw data, but that code is only executed when the system is first set up and once for each new attribute with a particular data distribution added to the identities in the future. The net run time to generate 100 K fake identities, inclusive of all distributional characteristics was 86 s on a standard desktop machine.

4.7. Mapping RNG Outputs to ID Characteristics

Each identity has its own set of PRNG outputs stored in a file indexed by the person's *UniqueID* attribute. The file consists of 256 × 32-bit integers that can be used in the initial generation of an identity or in assigning additional random attributes to fit future use cases. That flexibility supports post-generation incorporation of new attributes in a subset or all fake IDs. For each attribute, the ID-generating code takes the random numbers in sequence, applies the modulus operator by the size of the data set (thereby scaling the number to an appropriate size to access an index in the database), and the scaled value is then used to pull a document from the MongoDB database at the PN-derived index.

Pre-allocated bits of the PRNG outputs are assigned to each attribute. A process of masking the 32-bit numbers generated for each attribute is used as seen for Gender, Height, Weight and other attributes. By only using 8 or 16 bits of the 32-bit number for generating an index of the current dataset, we are future-proofing the fake ID by reserving the ability to insert larger lists with desired statistical characteristics. The remaining PRNG output words are reserved for future assignment of any new attribute of interest for the fake IDs.

4.8. Fake ID Construction Process

The high-level process of identity generation is captured in Figure 5. It begins with the inputs of files containing PRNG outputs and sets of raw data in MongoDB that contain all possible options for each attribute of identity. The ID Generating Python Script takes these two inputs and maps the appropriate random numbers to the collections in MongoDB, scaling them by the size of the collection and pulling a randomly selected value out of the collection based on its index. Once every attribute is added, a document containing all the information is inserted into the final FakeID database in a JSON format.

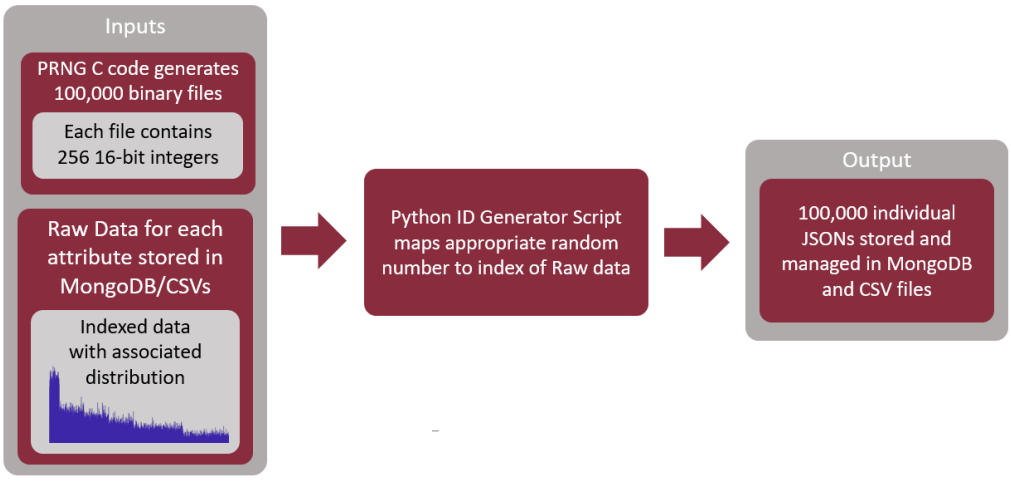

Figure 5. Overview of fake ID generation flow.

The fake ID database is set up with an API to retrieve information for future assignments as shown in Figure 6. The first method *getIDBufferArray* retrieves the sequenced PRNG output binary file and stores it in an array. The *getValue* and *getRange* method

calls represent generic calls that can be made to the sets of raw data retrieving a value at a chosen index and size of the dataset, respectively. The non-generic getters assign specific attributes that require a higher degree of control over which identities are assigned those attributes. The *Scale by collection* and *Scale by Numbers* are functions that scale the PRNG outputs retrieved from the buffer array by the size of the collection the number is being applied to ensure that the final index is always within the bounds of the raw data.

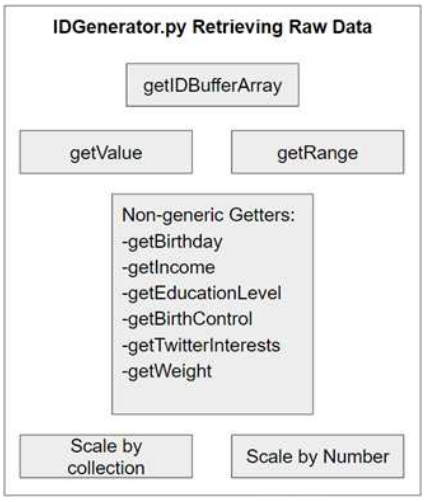

Figure 6. Method calls that enable access to the collection of fake identities.

While not all of the data retrieved by these methods will be used by every fake identity (i.e., *getTwitterInterests* is only used by accounts that sign up for Twitter or have a linked account), every single identity will be equally robust and flexible to meet the needs of different research questions. Generating passwords for the identities is also a unique category. There is utility in being able to manipulate the kinds of passwords generated randomly for each identity. As the uses of identities expand and more passwords or characteristics are generated, the length of the password as well as the type of normal and special characters used in the password can be changed. This is conducted primarily to adhere to different password requirements for the broad spectrum of online accounts to which fake identities will be assigned. Mechanically, such changes are handled as logged updates to the MongoDB database, so a level of bookkeeping is required to regenerate the fake identity once the database is allowed to become a living repository.

4.9. Storing and Managing Fake IDs

The PRNG code and ID-generating script are only run once at project start, and all subsequent updates or changes to the database are handled through a Python API. The API allows researchers to quickly query the database or add new attributes for future research questions. The API is written as a simple argparser utilizing a command line interface that can take "write" or "search" commands to either edit or query the database. Once a query is executed, the API will display the results and, if an additional user flag was added to the command, the results of the query will be written to a JSON file. Once the fake identities are used in an experiment, changes are frozen to administrative-only accesses. Additionally, a change log of all commands is also retained.

The API simply calls a host of different methods like *getIDByCriteria* or *getValueByCriteria*. The first returns the unique sequential identifier of identities that have a field that matches the value being sought, and the second retrieves the full identity with a specific field value that matches the search criteria. Each method logs that the query or write was completed, including which details were searched or edited. Maintaining the integrity of the dataset is vitally important to organizing data collection and processing. To ensure the data are protected and recoverable, several mitigation measures were put in place, beginning with the robust PRNG process and change logs. Should any identity data be corrupted

and need to be recovered, the PRNG with the same seed and identity-generating Python script can regenerate every identity or only single identities. We also utilize MongoDB's built-in user validation to mitigate human error. Finally, making and tracking changes through the API guarantees previous versions of the data are recoverable.

4.10. Preliminary Validation of Fake IDs

To ensure that the attributes on the IDs matched their respective distributions expected for each attribute, the output of the PRNG was first validated with Matlab as producing uniform random numbers, followed by statistical analysis of each attribute according to their programmed distributions. An example of the income distribution, which was based upon a derived distribution of (1) income range selection based upon published averages, followed by (2) uniform distribution within those proportionally chosen ranges is shown in Figure 7.

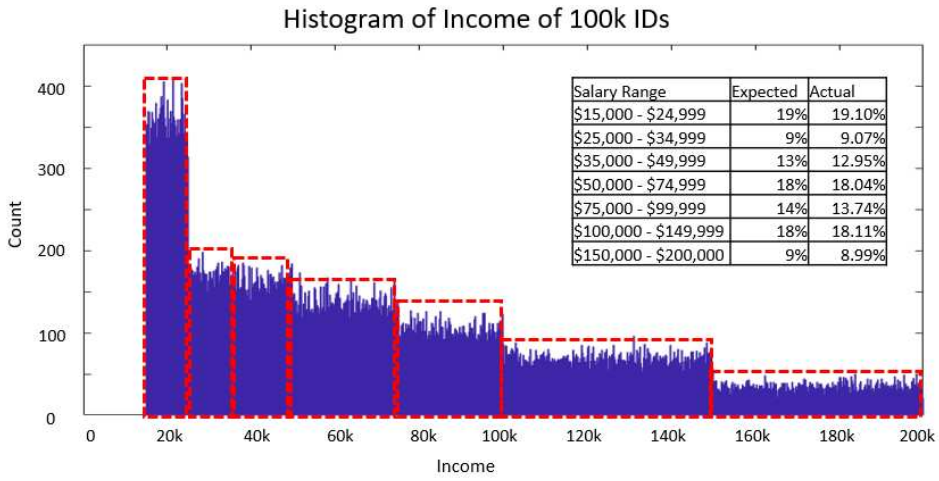

Figure 7. Histogram of the *Income* attribute of all 100K IDs plotted in Matlab.

The amount of occurrences of each attribute was evaluated independently to ensure proper mapping. While this is not a perfect process, the results confirm that each attribute matches their chosen distributions; as with any pseudorandom system, the results vary run-to-run. In rare cases where a skew in the distribution was noted, most often being from the mapping of PRNG values across mixed-radix domains [107], adjusting the number of random bits allocated to that attribute was sufficient to achieve the desired mapping. As the scale of the Use and Abuse project grew larger, the validation process was shifted to an automated read of attributes as contained in database records, enabling differential controls of distributions across blocks of IDs as desired.

Finally, there remains a question of how well the identities perform when assigned and used in an experiment. As an anecdotal example, our largest ongoing experiment included signing up identities for content sent by each of the nearly 2000 candidates (pre-primary) for upcoming U.S. elections; only one candidate (John Liccione of Florida's 13th district) has knowingly flagged an identity as fake, and there only by tracing the IP address back to Blacksburg, VA (IP obfuscation is a future addition to [11]). We will know more about the efficacy of the identities in that experiment in future months.

5. Use and Extension of Fake ID Generation

After creating an effective fake identity, researchers can use the identity to perform online experimentation and research while mitigating the ethical concerns associated with real human data. The identities can be signed up to websites or organizations where data can be collected and analyzed to answer research questions. The characteristics of fake identities can be tailored for various internet application purposes, as illustrated by the application categories and their required capabilities identified in Tables 1 and 2. Those

tailored fake identities can then be employed to answer questions such as those identified in Section 2.

Although the fake identities described so far are rich in their documentable attributes, a variety of extensions have been identified using broader toolsets. These include:

- Harness AI tools to create a fake person's image/video and activity more realistic.

To avoid accidental misuse of anyone's identity, and to provide a realistic online presence, AI-generated images or videos in the future could improve a fake ID's ability to stand up to human scrutiny. AI language and image models are already being utilized for both the propagation of and defense against malicious fake accounts online, and this technology will likely become a necessity, though our initial survey shows that only online social media, which invests heavily in prevention tools [135,136] presently looks for this content. At present, we believe that the detection capabilities are winning this competition, and thus have steered away from probing social media sites.

- Employ PO Box forwarding services provided by USPS to send and receive mail.

Our ongoing experiments show a surprising lack of activity for direct mail addressed to our fake accounts (real mailing addresses that we control), though some future experiments will seek to create convincing online identities anchored in the physical world that can stand up to automated and human scrutiny to a very high degree. Additionally, we have identified mail forwarding services in each state that would support the establishment of real addresses when desired.

- Create an account interaction engine to automate identity behaviors.

To truly target the identities and intent of suspicious content received, our fake IDs must have the ability to interact in a convincing manner. Many characteristics identified in Table 2, such as content interaction and scrolling, require an automated interaction method to complete at scale. The core of this capability is an *Account Interaction Engine* that selectively chooses based on identity to respond, click links, or open attachments (all within secure virtual machine infrastructures). Given that the interaction represents an opportunity to respond to received content, we intend to revisit the ethical considerations as we transition to a fully active OSINT platform.

- Use of fake IDs in social science research

The model of fake identities discussed here has been validated as efficacious through a variety of quantitative social science efforts, ranging from probing a subset of Beall's/Kscien's lists of suspected predatory publishers, predicting election results, or even quantifying policies and differential access to birth control by state. Future efforts will explore topics as far removed from the computer science foundations of the collection engine as theology.

6. Conclusions

As part of a broader effort to track how personal information is shared by online entities, this paper has performed a deep dive into the robust and repeatable generation of fake identities. Research shows that collecting information through fake online accounts organized by a single source has distinct advantages over what can normally be discovered in the public domain. This presents some challenges, however, as countermeasures to prevent fake account activity online continue to be developed and implemented. Certain characteristics tend to flag fake accounts as they are created or used. Most models are trained to detect bots at scale from a malicious source, and utilizing fake accounts in a benign manner could avoid detection for research purposes. The ethical ramifications of using fake identities can be managed by ensuring that PI is transmitted and never received, limiting the activity of fake users to have minimal impact on external systems, and ensuring that we only establish identities relevant to the underlying OSINT research problem.

As demonstrated through the previous Use and Abuse effort and related works, the utilization of fake accounts for privacy research can allow researchers to collect valuable

data about PI usage, while mitigating the ethical concerns surrounding real, human data. The Use and Abuse is a large-scale research project that seeks to employ fake identities to answer privacy-driven research questions about the propagation of personal data over the Internet. Moreover, the breadth of addressable problems using this infrastructure makes the centralized collection approach very valuable. Through a literature review of fake account generation and detection works, along with various works focusing on privacy research, a comprehensive model of digital characteristics for fake accounts was formed. This paper highlights the design and use of the fake ID attributes that enable the construction of realistic fake personas.

The backgrounds of each identity are rich enough to be extensible to many research questions both on the individual and larger demographic scales. The identities generated are customizable and can be tailored to various internet applications and domains, allowing for more in-depth data collection. Through this paper, benefits were outlined for using fake accounts for privacy research, a model for realistic fake identities was formed, and a repeatable generation process for IDs was created. The rich background of each individual and the unique process used to assemble each person in a consistent and convincing manner serve to improve the data gathered through the research project as well as serve as a defense against detection when operating online. The U&A project is unique both in terms of its scale and robust data-gathering method, utilizing semi-automated fake accounts to track complicated data-sharing behaviors.

Author Contributions: Conceptualization, A.M.; methodology, A.J.M.; software, E.H., J.K., C.H. and E.R.; validation, C.H., E.H., J.K. and E.R.; data curation, C.H. and E.R.; writing—original draft preparation, J.K., E.H., C.H., M.B. and A.J.M.; writing—review and editing, A.J.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data from these privacy experiments, including the fake identities, records of which fake identities were used to make one-time transactions, and all content received (email, phone, SMS text) is planned for release in 2026.

Acknowledgments: This work was supported in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit www.cyberinitiative.org. Additional support was also received from the VT National Security Institute's Spectrum Dominance Division, Raytheon Technologies, and ClearlyIP. Additionally, this material is based upon work supported by the National Science Foundation under Grants Number 1946493. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Michaels, A.J.; George, K.B. Use and Abuse of Personal Information. 2021. Available online: https://www.blackhat.com/us-21/briefings/schedule/#use--abuse-of-personal-information-22688 (accessed on 9 July 2024).
2. Harrison, J.; Lyons, J.; Anderson, L.; Maunder, L.; O'Donnell, P.; George, K.B.; Michaels, A.J. Quantifying Use and Abuse of Personal Information. In Proceedings of the 2021 IEEE International Conference on Intelligence and Security Informatics (ISI), San Antonio, TX, USA, 2–3 November 2021; IEEE: Piscataway, New Jersey, USA; 2021; pp. 1–6. [CrossRef]
3. Cranor, L.F.; LaMacchia, B.A. Spam! *Commun. ACM* **1998**, *41*, 74–83. [CrossRef]
4. Roesner, F.; Kohno, T.; Wetherall, D. Detecting and Defending Against Third-Party Tracking on the Web. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12), San Jose, CA, USA, 25–27 April 2012; pp. 155–168. Available online: https://www.usenix.org/conference/nsdi12/technical-sessions/presentation/roesner (accessed on 9 July 2024).
5. Nguyen, T.; Yeates, G.; Ly, T.; Albalawi, U. A Study on Exploring the Level of Awareness of Privacy Concerns and Risks. *Appl. Sci.* **2023**, *13*, 3237. [CrossRef]

6. Kost, E. 10 Biggest Data Breaches in Finance. 2023. Available online: https://www.upguard.com/blog/biggest-data-breaches-financial-services (accessed on 29 May 2024).
7. Shoop, T. OPM To Send Data Breach Notifications to Federal Employees Next Week. 2015. Available online: https://www.govexec.com/technology/2015/06/opm-send-data-breach-notifications-federal-employees-next-week/114556/ (accessed on 29 May 2024).
8. Ekran System. 7 Examples of Real-Life Data Breaches Caused by Insider Threats. 2023. Available online: https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches (accessed on 29 May 2024).
9. Clement, N. M&A Effect on Data Breaches in Hospitals: 2010–2022. In Proceedings of the 22nd Workshop on the Economics of Information Security, Geneva, Switzerland, 5–8 July 2023; pp. 1–63.
10. Ablon, L.; Heaton, P.; Lavery, D.C.; Romanosky, S. *Consumer Attitudes towards Data Breach Notifications and Loss of Personal Information*; Technical Report 1187; RAND Corporation: Santa Monica, CA, USA, 2016. Available online: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf (accessed on 9 July 2024).
11. Rheault, E.; Nerayo, M.; Leonard, J.; Kolenbrander, J.; Henshaw, C.; Boswell, M.; Michaels, A. Design of a Scalable OSINT Collection Engine. *J. Cybersecur. Privacy Spec. Issue Build. Community Good Pract. Cybersecur.* 2024.
12. Sigmund, T. Attention Paid to Privacy Policy Statements. *Digit. Econ. Soc. Inf. Manag.* **2021**, *12*, 144. [CrossRef]
13. Barth, S.; Ionita, D.; Hartel, P. Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines. *ACM Comput. Surv.* **2022**, *55*, 63. [CrossRef]
14. Fabian, B.; Ermakova, T.; Lentz, T. Large-scale readability analysis of privacy policies. In *WI '17: Proceedings of the International Conference on Web Intelligence, Leipzig, Germany, 23–26 August 2017*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 18–25. [CrossRef]
15. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report. 1979. Available online: https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html (accessed on 9 July 2024).
16. World Medical Association. World Medical Association Declaration of Helsinki: Ethical principles for medical research involving human subjects. *Bull. World Health Organ.* **2001**, *79*, 373–374. Available online: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/ (accessed on 9 July 2024).
17. Favaretto, M.; De Clercq, E.; Gaab, J.; Elger, B.S. First do no harm: An exploration of researchers' ethics of conduct in Big Data behavioral studies. *PLoS ONE* **2020**, *15*, e0241865. [CrossRef]
18. Mittelstadt, B.D.; Floridi, L. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci. Eng. Ethics* **2016**, *22*, 303–341. [CrossRef] [PubMed]
19. Daries, J.P.; Reich, J.; Waldo, J.; Young, E.M.; Whittinghill, J.; Ho, A.D.; Seaton, D.T.; Chuang, I. Privacy, anonymity, and big data in the social sciences. *Commun. ACM* **2014**, *57*, 56–63. [CrossRef]
20. O'Donnell, P.; Harrison, J.; Lyons, J.; Anderson, L.; Maunder, L.; Ramboyong, S.; Michaels, A.J. Quantitative Rubric for Privacy Policy Analysis. In Proceedings of the Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2021 International Workshops, DPM 2021 and CBT 2021, Darmstadt, Germany, 8 October 2021; Revised Selected Papers, Berlin/Heidelberg, Germany, 2021; pp. 39–54. [CrossRef]
21. Burattin, A.; Cascavilla, G.; Conti, M. SocialSpy: Browsing (Supposedly) Hidden Information in Online Social Networks. In *Proceedings of the Risks and Security of Internet and Systems*; Lopez, J., Ray, I., Crispo, B., Eds.; Springer: Cham, Switzerland, 2015; pp. 83–99. [CrossRef]
22. Elovici, Y.; Herzberg, A.; Fire, M. Ethical Considerations when Employing Fake Identities in Online Social Networks for Research. *Sci. Eng. Ethics* **2014**, *20*, 1027–1043. [CrossRef]
23. Luo, W.; Xie, Q.; Hengartner, U. FaceCloak: An Architecture for User Privacy on Social Networking Sites. In Proceedings of the 2009 International Conference on Computational Science and Engineering, Vancouver, BC, Canada, 29–31 August 2009; Volume 3, pp. 26–33. [CrossRef]
24. Sarikakis, K.; Winter, L. Social Media Users' Legal Consciousness About Privacy. *Soc. Media Soc.* **2017**, *3*, 1–14. [CrossRef]
25. Fahmy, S.G.; Abdelgaber, K.M.; Karam, O.H.; Elzanfaly, D.S. Modeling the Influence of Fake Accounts on User Behavior and Information Diffusion in Online Social Networks. *Informatics* **2023**, *10*, 27. [CrossRef]
26. Adewole, K.S.; Anuar, N.B.; Kamsin, A.; Varathan, K.D.; Razak, S.A. Malicious accounts: Dark of the social networks. *J. Netw. Comput. Appl.* **2017**, *79*, 41–67. [CrossRef]
27. Kantartopoulos, P.; Pitropakis, N.; Mylonas, A.; Kylilis, N. Exploring Adversarial Attacks and Defences for Fake Twitter Account Detection. *Technologies* **2020**, *8*, 64. [CrossRef]
28. Breuer, A.; Khosravani, N.; Tingley, M.; Cottel, B. Preemptive Detection of Fake Accounts on Social Networks via Multi-Class Preferential Attachment Classifiers. In *KDD '23 Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Long Beach, CA, USA, 6–10 August 2023*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 105–116. [CrossRef]
29. Elishar, A.; Fire, M.; Kagan, D.; Elovici, Y. Organizational Intrusion: Organization Mining Using Socialbots. In Proceedings of the 2012 International Conference on Social Informatics, Alexandria, VA, USA, 14–16 December 2012; pp. 7–12. [CrossRef]

30. Bos, N.; Karahalios, K.; Musgrove-Chávez, M.; Poole, E.S.; Thomas, J.C.; Yardi, S. Research ethics in the facebook era. In *CHI '09: Proceedings of the CHI Conference on Human Factors in Computing Systems, Boston, MA, USA, 4–9 April 2009*; Association for Computing Machinery: New York, NY, USA, 2009; pp. 2767–2770. [CrossRef]
31. Bilge, L.; Strufe, T.; Balzarotti, D.; Kirda, E. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In Proceedings of the 18th International Conference on World Wide Web, Madrid, Spain, 20–24 April 2009; Association for Computing Machinery: New York, NY, USA, 2009; WWW '09, pp. 551–560. [CrossRef]
32. Moreno, M.A.; Goniu, N.; Moreno, P.S.; Diekema, D. Ethics of Social Media Research: Common Concerns and Practical Considerations. *Cyberpsychol. Behav. Soc. Netw.* **2013**, *16*, 708–713. [CrossRef] [PubMed]
33. Homeland Security Public-Private Analytic Exchange Program. Ethics & OSINT Scorecard. Available online: https://www.dhs.gov/sites/default/files/2023-09/23_0829_oia_Ethics-OSINT-Scorecard_508.pdf (accessed on 8 July 2024).
34. Ma, X.; Andalibi, N.; Barkhuus, L.; Naaman, M. "People Are Either Too Fake or Too Real": Opportunities and Challenges in Tie-Based Anonymity. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, Denver, CO, USA, 5–11 May 2017; Association for Computing Machinery: New York, NY, USA, 2017; CHI '17, pp. 1781–1793. [CrossRef]
35. Chang, K.C.; Barber, S. Personalized Privacy Assistant: Identity Construction and Privacy in the Internet of Things. *Entropy* **2023**, *25*, 717. [CrossRef] [PubMed]
36. Aïmeur, E.; Schőnfeld, D. The ultimate invasion of privacy: Identity theft. In Proceedings of the 2011 Ninth Annual International Conference on Privacy, Security and Trust, Montreal, QC, Canada, 19–21 July 2011; pp. 24–31. [CrossRef]
37. Shafahi, M.; Kempers, L.; Afsarmanesh, H. Phishing Through Social Bots on Twitter. In Proceedings of the IEEE International Conference on Big Data, Amsterdam, Orlando, FL, USA, 5–9 December 2016; pp. 3703–3712. [CrossRef]
38. EU Panel for the Future of Science and Technology. Polarisation and the Use of Technology in Political Campaigns and Communication. Technical Report PE 634.414. 2019. Available online: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2019)634414 (accessed on 9 July 2024).
39. Zannettou, S.; Caulfield, T.; Bradlyn, B.; De Cristofaro, E.; Stringhini, G.; Blackburn, J. Characterizing the Use of Images in State-Sponsored Information Warfare Operations by Russian Trolls on Twitter. *Proc. Int. AAAI Conf. Web Soc. Media* **2020**, *14*, 774–785. [CrossRef]
40. Hakak, S.; Khan, W.; Bhattacharya, S.; Gadekallu, T.; Choo, K.K.R. Propagation of Fake News on Social Media: Challenges and Opportunities. In Proceedings of the Computational Data and Social Networks: 9th International Conference, CSoNet 2020, Dallas, TX, USA, 11–13 December 2020; Proceedings 9; Springer: Cham, Switzerland, 2020; pp. 345–353 [CrossRef]
41. Puleri, J. Law Enforcement and Open Source Intelligence: Evolution, Technologies, and Privacy Issues. Ph.D. Thesis, Utica College, Utica, NY, USA, 2021.
42. Suriadi, S.; Foo, E.; Smith, J. Chapter 4—Enhancing Privacy to Defeat Open Source Intelligence. In *Automating Open Source Intelligence*; Layton, R., Watters, P.A., Eds.; Syngress: Boston, MA, USA, 2016; pp. 61–78. [CrossRef]
43. Hayes, D.R.; Cappa, F. Open-source intelligence for risk assessment. *Bus. Horizons* **2018**, *61*, 689–697. [CrossRef]
44. Shaikh, O. Detection and Classification of Personally Identifiable Information in Images Using Artificial Intelligence. *TechRxiv* **2024**, 1–6. [CrossRef]
45. Arefi, M.N.; Alexander, G.; Crandall, J.R. PIITracker: Automatic Tracking of Personally Identifiable Information in Windows. In Proceedings of the 11th European Workshop on Systems Security, Porto, Portugal, 23–26 April 2018; EuroSec'18. [CrossRef]
46. Fugkeaw, S.; Worapaluk, K.; Tuekla, A.; Namkeatsakul, S. Design and Development of a Dynamic and Efficient PII Data Loss Prevention System. In *Proceedings of the Recent Advances in Information and Communication Technology 2021*; Meesad, P., Sodsee, D.S., Jitsakul, W., Tangwannawit, S., Eds.; Springer: Cham, Switzerland, 2021; pp. 23–33.
47. Dao, H.; Fukuda, K. Alternative to third-party cookies: Investigating persistent PII leakage-based web tracking. In Proceedings of the 17th International Conference on Emerging Networking EXperiments and Technologies, Virtual Event, Germany, 7–10 December 2021; CoNEXT '21; pp. 223–229. [CrossRef]
48. Ren, J.; Rao, A.; Lindorfer, M.; Legout, A.; Choffnes, D. ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, Singapore, 26–30 June 2016; MobiSys '16; pp. 361–374. [CrossRef]
49. Krishnamurthy, B.; Wills, C.E. On the leakage of personally identifiable information via online social networks. In Proceedings of the 2nd ACM Workshop on Online Social Networks, Barcelona, Spain, 17 August 2009; WOSN '09; pp. 7–12. [CrossRef]
50. Venkatadri, G.; Andreou, A.; Liu, Y.; Mislove, A.; Gummadi, K.P.; Loiseau, P.; Goga, O. Privacy Risks with Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018; pp. 89–107. [CrossRef]
51. Malheiros, M.; Jennett, C.; Patel, S.; Brostoff, S.; Sasse, M.A. Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Austin, TX, USA, 5–10 May 2012; CHI '12, pp. 579–588. [CrossRef]
52. Gates, M. Frankenstein Fraud: How Synthetic Identities Became the Fastest-Growing Fraud Trend. *Security Management*. 2021. Available online: https://www.asisonline.org/security-management-magazine/articles/2021/05/frankenstein-fraud-how-synthetic-identities-became-the-fastest-growing-fraud-trend/ (accessed on 9 July 2024).
53. Teixeira da Silva, J.A. Fake peer reviews, fake identities, fake accounts, fake data: Beware! *AME Med. J.* **2017**, *2*, 1–4. [CrossRef]

54. Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. The socialbot network: When bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, Orlando, FL, USA, 5–9 December 2011; ACSAC '11, pp. 93–102. [CrossRef]
55. Pathak, A. An Analysis of Various Tools, Methods and Systems to Generate Fake Accounts for Social Media. Master's Thesis, Northeastern University, Boston, MA, USA, 2014.
56. Fatema, A.S.; Mattar, E.A. Recent advances in artificial intelligence techniques for identifying fake accounts: A review. In Proceedings of the 6th Smart Cities Symposium (SCS 2022), Hybrid Conference, Bahrain, 6–8 December 2022; Volume 2022, pp. 504–507. [CrossRef]
57. Masood, F.; Ammad, G.; Almogren, A.; Abbas, A.; Khattak, H.A.; Ud Din, I.; Guizani, M.; Zuair, M. Spammer Detection and Fake User Identification on Social Networks. *IEEE Access* **2019**, *7*, 68140–68152. [CrossRef]
58. Baccarella, C.V.; Wagner, T.F.; Kietzmann, J.H.; McCarthy, I.P. Social media? It's serious! Understanding the dark side of social media. *Eur. Manag. J.* **2018**, *36*, 431–438. [CrossRef]
59. Anklesaria, K.; Desai, Z.; Kulkarni, V.; Balasubramaniam, H. A Survey on Machine Learning Algorithms for Detecting Fake Instagram Accounts. In Proceedings of the 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 17–18 December 2021; pp. 141–144. [CrossRef]
60. Gurajala, S.; White, J.; Hudson, B.; Voter, B.; Matthews, J. Profile characteristics of fake Twitter accounts. *Big Data Soc.* **2016**, *3*. [CrossRef]
61. Xiao, C.; Freeman, D.M.; Hwa, T. Detecting Clusters of Fake Accounts in Online Social Networks. In Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security, Denver, CO, USA, 16 October 2015; AISec '15, pp. 91–101. [CrossRef]
62. Sarode, A.J.; Mishra, A. Audit and Analysis of Impostors: An experimental approach to detect fake profile in online social network. In Proceedings of the Sixth International Conference on Computer and Communication Technology 2015, Allahabad, India, 25–27 September 2015; ICCCT '15; pp. 1–8. [CrossRef]
63. Kozlov, F.; Yuen, I.; Kowalczyk, J.; Bernhardt, D.; Freeman, D.; Pearce, P.; Ivanov, I. Evaluating Changes to Fake Account Verification Systems. In Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020), San Sebastian, Spain, 14–16 October 2020; pp. 135–148. Available online: https://www.usenix.org/conference/raid2020/presentation/kozlov (accessed on 9 July 2024).
64. Staddon, J.; Huffaker, D.; Brown, L.; Sedley, A. Are privacy concerns a turn-off? engagement and privacy in social networks. In Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, USA, 11–13 July 2012; SOUPS '12. [CrossRef]
65. Kulkarni, V.; Aashritha Reddy, D.; Sreevani, P.; Teja, R. Fake profile identification using ANN. In Proceedings of the 4th Smart Cities Symposium (SCS 2021), Online, 21–23 November 2021; Volume 2021, pp. 375–380. [CrossRef]
66. Fire, M.; Kagan, D.; Elyashar, A.; Elovici, Y. Friend or foe? Fake profile identification in online social networks. *Soc. Netw. Anal. Min.* **2013**, *4*, 194. [CrossRef]
67. Gross, R.; Acquisti, A. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7 November 2005; WPES '05, pp. 71–80. [CrossRef]
68. Borkar, B.S.; Patil, D.R.; Markad, A.V.; Sharma, M. Real or Fake Identity Deception of Social Media Accounts using Recurrent Neural Network. In Proceedings of the 2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP), Uttarakhand, India, 23–24 November 2022; pp. 80–84. [CrossRef]
69. Jain, P.; Gyanchandani, M.; Khare, N. Big data privacy: A technological perspective and review. *J. Big Data* **2016**, *3*, 25. [CrossRef]
70. Boshmaf, Y.; Ripeanu, M.; Beznosov, K.; Santos-Neto, E. Thwarting Fake OSN Accounts by Predicting their Victims. In Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security, Denver, CO, USA, 16 October 2015; AISec '15, pp. 81–89. [CrossRef]
71. Elyusufi, Y.; Elyusufi, Z.; Kbir, M.A. Social networks fake profiles detection based on account setting and activity. In Proceedings of the 4th International Conference on Smart City Applications, Casablanca, Morocco, 2–4 October 2019; SCA '19. [CrossRef]
72. Sowmya, P.; Chatterjee, M. Detection of Fake and Clone accounts in Twitter using Classification and Distance Measure Algorithms. In Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 28–30 July 2020; pp. 0067–0070. [CrossRef]
73. Wanda, P. RunMax: Fake profile classification using novel nonlinear activation in CNN. *Soc. Netw. Anal. Min.* **2022**, *12*, 158. [CrossRef]
74. Kuhn, M.L. 147 Million Social Security Numbers for Sale: Developing Data Protection Legislation after Mass Cybersecurity Breaches. *Iowa Law Rev.* **2018**, *104*. Available online: https://ilr.law.uiowa.edu/print/volume-103-issue-6/147-million-social-security-numbers-for-sale-developing-data-protection-legislation-after-mass-cybersecurity-breaches (accessed on 9 July 2024).
75. Singh, V.; Shanmugam, R.; Awasthi, S. Preventing Fake Accounts on Social Media Using Face Recognition Based on Convolutional Neural Network. In *Proceedings of the Sustainable Communication Networks and Application*; Karuppusamy, P., Perikos, I., Shi, F., Nguyen, T.N., Eds.; Springer: Singapore, 2021; pp. 227–241. [CrossRef]
76. Benabbou, F.; Boukhouima, H.; Sael, N. Fake accounts detection system based on bidirectional gated recurrent unit neural network. *Int. J. Electr. Comput. Eng. (IJECE)* **2022**, *12*, 3129. [CrossRef]
77. Khaled, S.; El-Tazi, N.; Mokhtar, H.M.O. Detecting Fake Accounts on Social Media. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 3672–3681. [CrossRef]

78. Caruccio, L.; Desiato, D.; Polese, G. Fake Account Identification in Social Networks. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5078–5085. [CrossRef]
79. Muñoz, S.D.; Paul Guillén Pinto, E. A dataset for the detection of fake profiles on social networking services. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 230–237. [CrossRef]
80. Asghari, S.; Chehreghani, M.H.; Chehreghani, M.H. On Using Node Indices and Their Correlations for Fake Account Detection. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022; pp. 5656–5661. [CrossRef]
81. Liang, X.; Yang, Z.; Wang, B.; Hu, S.; Yang, Z.; Yuan, D.; Gong, N.Z.; Li, Q.; He, F. Unveiling Fake Accounts at the Time of Registration: An Unsupervised Approach. In Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining, Singapore, 14–18 August 2021; KDD '21, pp. 3240–3250. [CrossRef]
82. McDonald, A.; Sugatan, C.; Guberek, T.; Schaub, F. The Annoying, the Disturbing, and the Weird: Challenges with Phone Numbers as Identifiers and Phone Number Recycling. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2021; CHI '21. [CrossRef]
83. Mulliner, C. Privacy leaks in mobile phone internet access. In Proceedings of the 2010 14th International Conference on Intelligence in Next Generation Networks, Berlin, Germany, 11–14 October 2010; pp. 1–6. [CrossRef]
84. Baglioni, E.; Becchetti, L.; Bergamini, L.; Colesanti, U.; Filipponi, L.; Vitaletti, A.; Persiano, G. A lightweight privacy preserving SMS-based recommendation system for mobile users. In Proceedings of the Fourth ACM Conference on Recommender Systems, Barcelona, Spain, 26–30 September 2010; RecSys '10, pp. 191–198. [CrossRef]
85. Lucas, M.M.; Borisov, N. FlyByNight: Mitigating the privacy risks of social networking. In Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 27 October 2008; WPES '08, pp. 1–8. [CrossRef]
86. Akyon, F.C.; Esat Kalfaoglu, M. Instagram Fake and Automated Account Detection. In Proceedings of the 2019 Innovations in Intelligent Systems and Applications Conference (ASYU), Izmir, Turkey, 31 October–2 November 2019; pp. 1–7. [CrossRef]
87. El Haddad, G.; Aïmeur, E.; Hage, H. Understanding Trust, Privacy and Financial Fears in Online Payment. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing And Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 28–36. [CrossRef]
88. Sahi, A.M.; Khalid, H.; Abbas, A.F.; Zedan, K.; Khatib, S.F.A.; Al Amosh, H. The Research Trend of Security and Privacy in Digital Payment. *Informatics* **2022**, *9*, 32. [CrossRef]
89. Antoniou, G.; Batten, L.; Narayan, S.; Parampalli, U. A Privacy Preserving E-Payment Scheme. In *Proceedings of the Intelligent Distributed Computing III*; Papadopoulos, G.A., Badica, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 197–202.
90. Florencio, D.; Herley, C. A large-scale study of web password habits. In Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada, 8–12 May 2007; WWW '07, pp. 657–666. [CrossRef]
91. Bhagavatula, S.; Bauer, L.; Kapadia, A. "Adulthood is trying each of the same six passwords that you use for everything": The Scarcity and Ambiguity of Security Advice on Social Media. *Proc. ACM Hum.-Comput. Interact. (PACM HCI)* **2022**, *6*; pp. 1–27. [CrossRef]
92. Darrow, J.J.; Lichtenstein, S.D. Do You Really Need My Social Security Number—Data Collection Practices in the Digital Age. *N. Carol. J. Law Technol.* **2008**, 1–59. Available online: https://scholarship.law.unc.edu/ncjolt/vol10/iss1/2 (accessed on 9 July 2024).
93. Roy, P.K.; Chahar, S. Fake Profile Detection on Social Networking Websites: A Comprehensive Review. *IEEE Trans. Artif. Intell.* **2020**, *1*, 271–285. [CrossRef]
94. Chen, Y.C.; Wu, S.F. FakeBuster: A Robust Fake Account Detection by Activity Analysis. In Proceedings of the 2018 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Taipei, Taiwan, 26–28 December 2018; pp. 108–110. [CrossRef]
95. Erşahin, B.; Aktaş, d.; Kılınç, D.; Akyol, C. Twitter fake account detection. In Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5–8 October 2017; pp. 388–392. [CrossRef]
96. Swe, M.M.; Nyein Myo, N. Fake Accounts Detection on Twitter Using Blacklist. In Proceedings of the 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore, 6–8 June 2018; pp. 562–566. [CrossRef]
97. Chakraborty, M.; Das, S.; Mamidi, R. Detection of Fake Users in Twitter Using Network Representation and NLP. In Proceedings of the 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 4–8 January 2022; pp. 754–758. [CrossRef]
98. Bharti, K.K.; Pandey, S. Fake account detection in twitter using logistic regression with particle swarm optimization. *Soft Comput.* **2021**, *25*, 11333–11345. [CrossRef]
99. Nikhitha, K.V.; Bhavya, K.; Nandini, D.U. Fake Account Detection on Social Media using Random Forest Classifier. In Proceedings of the 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 17–19 May 2023; pp. 806–811. [CrossRef]
100. Das, S.; Saha, S.; Vijayalakshmi, S.; Jaiswal, J. An Effecient Approach to Detect Fraud Instagram Accounts Using Supervised ML Algorithms. In Proceedings of the 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 16–17 December 2022; pp. 760–764. [CrossRef]

101. Goyal, B.; Gill, N.S.; Gulia, P.; Prakash, O.; Priyadarshini, I.; Sharma, R.; Obaid, A.J.; Yadav, K. Detection of Fake Accounts on Social Media Using Multimodal Data With Deep Learning. *IEEE Trans. Comput. Soc. Syst.* 2023, *early access*. [CrossRef]
102. Stolbova, A.; Ganeev, R.; Ivaschenko, A. Intelligent Identification of Fake Accounts on Social Media. In Proceedings of the 2021 30th Conference of Open Innovations Association FRUCT, Oulu, Finland, 27–29 October 2021; pp. 279–284. [CrossRef]
103. Breuer, A.; Eilat, R.; Weinsberg, U. Friend or Faux: Graph-Based Early Detection of Fake Accounts on Social Networks. In Proceedings of the Web Conference 2020, Taipei, Taiwan, 20–24 April 2020; WWW '20, pp. 1287–1297. [CrossRef]
104. Brook, C. PII Data Classification: 4 Best Practices. 2023. Available online: https://www.digitalguardian.com/blog/pii-data-classification-4-best-practices (accessed on 29 May 2024).
105. Michaels, A.J. A maximal entropy digital chaotic circuit. In Proceedings of the 2011 IEEE International Symposium of Circuits and Systems (ISCAS), Rio de Janeiro, Brazil, 15–18 May 2011; pp. 717–720. [CrossRef]
106. Michaels, A.J. Improved RNS-Based PRNGs. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; ARES 2018. [CrossRef]
107. Vennos, A.; Michaels, A. Shannon Entropy Loss in Mixed-Radix Conversions. *Entropy* **2021**, *23*, 967. [CrossRef] [PubMed]
108. US Census Bureau. Age and Sex Composition: 2010. Available online: https://www.census.gov/content/dam/Census/library/publications/2011/dec/c2010br-03.pdf (accessed on 29 May 2024).
109. US Social Security Administration. Popular Baby Names by Decade. Available online: https://www.ssa.gov/oact/babynames/limits.html (accessed on 29 May 2024).
110. US Census Bureau. Frequently Occurring Surnames. Available online: https://www.census.gov/topics/population/genealogy/data/2010_surnames.html (accessed on 29 May 2024).
111. US Census Bureau. National Population. Available online: https://www.census.gov/data/tables/time-series/demo/popest/2020s-national-detail.html (accessed on 29 May 2024).
112. US Census Bureau. State Population Totals. Available online: https://www.census.gov/data/tables/time-series/demo/popest/2020s-state-total.html (accessed on 29 May 2024).
113. OpenAddresses. Open Street Addresses. Available online: https://batch.openaddresses.io/data (accessed on 29 May 2024).
114. US Census Bureau. USPS. Available online: https://pypi.org/project/usps-api/ (accessed on 29 May 2024).
115. UC Santa Barbara. 2020 Election. Available online: https://www.presidency.ucsb.edu/statistics/elections/2020 (accessed on 29 May 2024).
116. Statista Research Department. Household Income 2021. Available online: https://www.statista.com/statistics/203183/percentage-distribution-of-household-income-in-the-us/ (accessed on 29 May 2024).
117. US Census Bureau. Educational Attainment Data. Available online: https://www.census.gov/newsroom/press-releases/2022/educational-attainment.html (accessed on 29 May 2024).
118. Statista. College Majors. Available online: https://cew.georgetown.edu/wp-content/uploads/Economic-Value-of-College-Majors-Full-Report-v2.compressed.pdf (accessed on 29 May 2024).
119. Gallup. Sexualities by Generation. Available online: https://news.gallup.com/poll/389792/lgbt-identification-ticks-up.aspx (accessed on 29 May 2024).
120. Centers for Disease Control. Body Measurements. Available online: https://www.cdc.gov/nchs/fastats/body-measurements.htm (accessed on 29 May 2024).
121. US Bureau of Labor Statistics. Employment by Detailed Occupation. Available online: https://www.bls.gov/emp/tables/emp-by-detailed-occupation.htm (accessed on 29 May 2024).
122. US Census Bureau. QuickFacts United States. Available online: https://www.census.gov/quickfacts/fact/table/US# (accessed on 29 May 2024).
123. Pew Research Center. Afro-Latino. Available online: https://www.pewresearch.org/short-reads/2022/05/02/about-6-million-u-s-adults-identify-as-afro-latino/ (accessed on 29 May 2024).
124. Pew Research Center. Key Facts about Asian Americans. Available online: https://www.pewresearch.org/short-reads/2021/04/29/key-facts-about-asian-americans/ (accessed on 29 May 2024).
125. Smarty. USPS and International Address Verification. 2023. Available online: https://www.smarty.com/articles/usps-address-verification (accessed on 29 May 2024).
126. Melissa Lookup. Address Search Tools. 2023. Available online: https://lookups.melissa.com/home/mapcart/zipcode/ (accessed on 29 May 2024).
127. Apostol, T.M. *Introduction to Analytic Number Theory*; Undergraduate Texts in Mathematics; Springer: Berlin/Heidelberg, Germany, 2010; pp. 1–352.
128. Abdulkader, H.; Samir, R.; Hussien, R. Improved RSA security using Chinese Remainder Theorem and Multiple Keys. *Future Comput. Inform. J.* **2019**, *4*, 1–60. [CrossRef]
129. Michaels, A.J.; Palukuru, V.S.S.; Fletcher, M.J.; Henshaw, C.; Williams, S.; Krauss, T.; Lawlis, J.; Moore, J.J. CAN Bus Message Authentication via Co-Channel RF Watermark. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3670–3686. [CrossRef]
130. McGinthy, J.M.; Michaels, A.J. Semi-Coherent Transmission Security for Low Power IoT Devices. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 170–177. [CrossRef]

131. Social Security Administration. Top Names of the 2010s. Available online: https://www.ssa.gov/oact/babynames/decades/names2010s.html (accessed on 29 May 2024).
132. US Census Bureau. County Population Totals and Components of Change: 2020–2023. 2023. Available online: https://www.census.gov/data/tables/time-series/demo/popest/2020s-counties-total.html (accessed on 29 May 2024).
133. Fryar, C.D.; Carroll, M.D.; Gu, Q.; Afful, J.; Ogden, C. Anthropometric Reference Data for Children and Adults: United States, 2015–2018. Technical Report, National Center For Health Statistics, Hayattsville, Maryland, 2021. Available online: https://stacks.cdc.gov/view/cdc/100478. (accessed on 9 July 2024).
134. Statista Research Department. Major Political Party Identification U.S. 2000–2023. Technical Report, Statista Research, 2024. Available online: https://www.statista.com/statistics/1078383/political-party-identification-in-the-us/ (accessed on 29 May 2024).
135. Kamruzzaman, M. Impact of Social Media on Geopolitics and Economic Growth: Mitigating the Risks by Developing Artificial Intelligence and Cognitive Computing Toolss. *Comput. Intell. Neurosci.* **2022**, *1*, 1–12. [CrossRef]
136. Yang, K.C.; Varol, O.; Davis, C.A.; Ferrara, E.; Flammini, A.; Menczer, F. Arming the public with artificial intelligence to counter social bots. Hum. Behav. Emerg. Technol. **2019**, *1*, 48–61. [CrossRef]