Authorized Representation as a Threat Under Privacy Regulations

Isaiah Genis
NYU Tandon
New York, NY
Isaiah.Genis@nyu.edu

***Abstract*— The focus of this research work is to analyze the problem of how legally valid data subject requests submitted by authorized representatives on behalf of data subjects in line with the General Data Protection Regulation and California Consumer Privacy Act are handled. We establish such a representative company for the purposes of evaluating company responses. Responses indicate that this use case is not properly factored into companies' compliance plans.**

Keywords—Privacy, California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR)

I. Introduction (*Heading 1*)

The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) are rules designed to help empower the ownership of your data, but research suggests these regulations can lead to additional harm and new attack vectors that impact both businesses and consumers. GDPR and CCPA both place stringent compliance timeframes on data subject requests. In order to facilitate compliance with these regulations and empower both businesses and consumers companies have arisen to help manage these requests and data. We assert that the rise of compliance assistance companies both for businesses and customers, in combination with many companies rush to meet regulatory timelines, or face fines, are promoting insufficient identity verification. Companies like BrandYourself, Deleteme, PrivacyBee and Mine submit requests outside of company specific portals using templated emails and make it easier for bad actors to and appear to have legitimacy and pretend to be acting on behalf of users. We take a similar approach to these companies and submit requests representing consenting subjects to track how these authorized representative requests are processed.

The organization of the paper is as follows. In section II we will define the related work on this topic. We will then review the use case and threat model we are considering. In section III we will review the related work and our methods used. In Section IV we will review the results.

II. Related Work

There has been some great analysis of the new threat landscape under new privacy regulations. Di Martino and Robyns review GDPR and identify incompatibilietes of legal vs technical compliance with GDPR that can lead to less security and privcacy for individuals. They find that there is a lack of uniform practice in handling these requests and that for almost 30% of companies examined they were able to impersonate a subject and get access to their data using only information found on social media and the like. They propose more standardized and sufficent authentication methods that cannot be beaten through open source intelligence. [1]

Pavur and Kneer focused on how large a problem this may be by applying a similar methodolgy as used by Di Martino, et al; but applying it to over three times the sample size of companies and using a similar looking address rather than spoofing the users true email address. They limited their working knowledge of subject to Open-source intelligence. Pavur and Knerr focus on unsophisticated attacks that only rely on email and simple forgery of documents. They were able to validate that approximately 25% provided sensitive verification based on their request without verifying the requester and another 15% that could be easily fooled. [2]

Cagnazzo et al focused on the less thought of offline attacks to GDPR "letters". This low-tech approach, "is a general attack not exploiting a technical flaw, but rather an organizational and human protocol flaw." [3] They constructed a template Subject Access request led to the return of personal information by 10 out of 14 companies tested. [3]

Our work differs from others in two main factors. The first is that we are not attempting to directly impersonate the data subject, but are asserting we are an authorized representative of the subject similar to how PrivacyBee and others submit their requests. Secondly our work differs by including consideration for the California Cosnumer Privacy Act and companies that may have not been subject to GDPR.

III. Threat Model

A. *Identifying our Threats*

There are several threats that can face both data subject and companies under GDPR and CCPA. We concern ourselves with those that can be associated with attempts

related to impersonation of an authorized agent of the data subject. The most pressing concern to consumers is the unauthorized disclosure of personal information. The second most pressing concern to consumers is the authorized deletion of personal data at the request of a bad actor. The threats to companies include the unauthorized disclosure of data but can also include the increased cost associated with reviewing additional requests and processing additional potentially fraudulent requests and the opportunity cost of no longer having as much data for the company to leverage. [4]

B. *Classifying our threats*

Under the STRIDE Model the threat of deletion would be classified as Tampering and Denial of Service. Under STRIDE the threat of access would be a threat of Information Disclosure.

For a DREAD Analysis of the vulnerabilities, we apply OppenStack's DREAD Scoring Methodology (with each out of ten). [5]

- **Damage-10:** Data is destroyed, but it may be recoverable.
- **Reproducability-7:** The threats and attacks being reviewed rely on minimal skill and is not dissimilar from launching a phishing scam.
- **Exploitability-5:** We would require some data collection and storage as well as a few other resources to make this non-trivial, but it could be done in an automated or call-center like fashion.
- **Affected Users-6:** While each attack may only compromise a single user the same vulnerability and exploit can be repeated for countless others.
- **Discoverability-7:** This is a known issue with related works such as those referenced able to achieve success in a non-trivial percentage of cases, but there is a base level of knowledge and skill required to setup and identify targets.

IV. EMPIRICAL EVIDENCE

Following similar procedures to the related works and the companies we mention in our introduction we used a form email that was sent to 44 companies we believed to have data on the authorizing subject based on their email history. These emails were sent from a legally established LLC with a website and domain with written consent of the subject. Our form letter specified the request was deletion of data as we felt that was the must impactful threat to both the company and the user. Responses and actions were manual after initial actions but using as standardized language as possible and never attempting to say we are the user.

Of the 44 companies contacted 26 did not send any relevant response within the appropriate regulatory timeframes. Approximately 10% informed us that the listed username/email for the data subject was not found in their systems and another 10% required login to their system to submit/verify a request. 5 of the 44 deleted the subject's data almost immediately with no additional verification or action required other than the additional request.

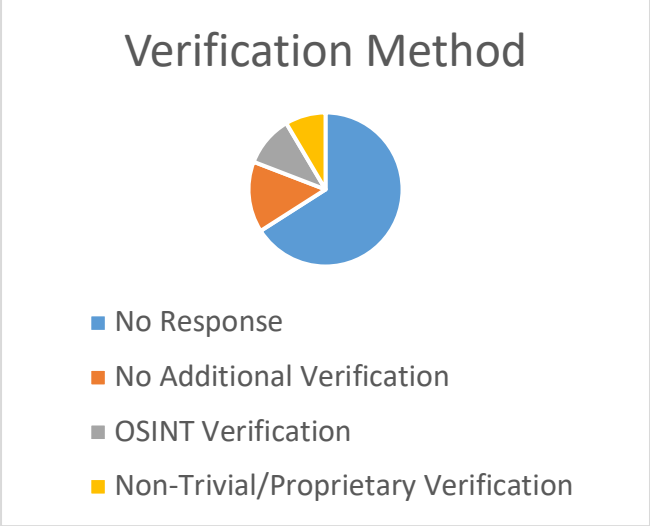

Figure IV-1

V. CONCLUSIONS AND FUTURE WORK

While Cagnazzo, et al may have had remarkable success with their alterative channel approach of offline letters; and Pavur and Kneer had a very high response rate our efforts were not as fruitful. We were extremely surprised to see such a high number companies fail to send any acknowledgement or response to our requests and that the overwhelming majority of responses received did not appear to acknowledge or have a response to handle that the request was not made by the data subject. Our response rate was significantly lower than those of the more direct impersonation efforts in the related works. It is possible these companies may be filtering their processing to only include emails from known account addresses or that they have suspended operations during the COVID-19 pandemic. The legal complexities and ever-changing landscape as exemplified by the Schrems II ruling this past summer indicate there is still much work to be done for companies to understand and fulfill their obligations. Any verification information other than login to the application or direct access to the email address listed on the account could easily have been fulfilled using OSINT. It appears many of the consumer facing privacy companies still have quite a bit of work ahead of them in order to become a recognized part of the system and company specific processes will continue to impede consumers' ability to regain control over their data.

Further work would include additional communication methods and attempts to get companies to handle our representative requests as well as work to negotiate an accepted verification method for representative requests.

ACKNOWLEDGMENT

Thank you, Professors Aspen Olmstead and Kevin Gallagher, and the entire NYU Cyber Fellows Cohort.

VI. REFRENCES

[1] M. D. Martino and P. Robyns, "Personal Information Leakage by Abusing the GDPR “Right of Access”," in *Fifteenth Symposium on Usable Privacy and Security*, Santa Clara, 2019.

[2] J. Pavur, "GDPArrrrr: Using Privacy Laws to Steal Identities," in *Black Hat USA*, 2019.

[3] M. Cagnazzo, "Gdpirated-stealing personal information on-and offline," in *European Symposium on Research in Computer Security*, 2019.

[4] BrandYouself, "BrandYourself Site," [Online]. Available: https://brandyourself.com. [Accessed 13 12 2020].

[5] OpenStack, "Security/OSSA-Metrics," [Online]. Available: https://wiki.openstack.org/wiki/Security/OSSA-Metrics. [Accessed October 2020].

[6] W. Stallings, "Handling of Personal Information and Deidentified, Aggregated and Pseudonymized Information Under the California Consumer PRivacy Act," *IEEE Security & Privacy,* vol. 18, no. 1, pp. 61-64, 2020.

[7] L. Bufalieri and M. L. Morgia, "GDPR: When the Right to Access Personal Data Becomes a Threat," in *IEEE INTERNATIONAL CONFERENCE ON WEB SERVICES (ICWS) 2020*, 2020.

[8] PrivacyBee, "PrivacyBee," [Online]. Available: https://privacybee.com/. [Accessed 13 12 2020].

[9] Abine, Inc, "DeleteMe Site," [Online]. Available: https://joindeleteme.com/. [Accessed 12 12 2020].