Undergraduate Thesis Prospectus

Preventing Machine Learning Models from Leaking Private Information
(technical research project in Computer Science)

Front-End Protection: How the General Data Protection Regulation Is Enforced
(sociotechnical research project)

by

Maclay Teefey

October 27, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Maclay Teefey

Technical advisor: Rosanne Vrugtman, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can online private information be protected?

Private information leaks have had large consequences for businesses and people whose data was leaked. In their 2022 report, IBM calculated that the average cost globally for a data breach was $4.35 million (IBM, 2022). Data leaks even threaten the lives of individuals involved, as shown with the Ashley Madison breach exposing the sexual relations of the users (Thielman, 2015). One user in Saudi Arabia emphasized the importance of the leak with his post to Reddit titled “I May Get Stoned to Death for Gay Sex (Gay Man from Saudi Arabia Who Used Ashley Madison for Hookups.)” in which he describes how he used Ashely Madison “to hook up with single guys” (ICouldBeStoned2Death, 2015). He states that “gay sex [being] punishable by death in my home country” and he had to leave Saudi Arabia permanently to avoid being killed (ICouldBeStoned2Death, 2015).

Preventing Machine Learning Models Leaking Private Information

How can machine learning models reduce private information leakage?

Machine learning models are not immune to data breaches. Researchers Arvind Narayanan and Vitaly Shmatikov exploited the failure of anonymization techniques for machine learning algorithms using micro-data with the Netflix Prize model as a case study (Narayanan & Shmatikov, 2008). They discovered that only “8 movie ratings (of which 2 may be completely wrong) and dates that may have a 14-day error, 99% of records can be uniquely identified in the dataset” (Narayanan & Shmatikov, 2008). Data leakage can even

occur as part of efforts to remove specific user data from machine learning models mandated by the General Data Protection Regulation (Zanella-Béguelin et al., 2020). Data leakage can be mitigated using state-of-the-art techniques including differential privacy and two-stage continued training, and are necessary for fields with legal consequences to private information being disclosed (Zanella-Béguelin et al., 2020).

My technical research project will be in the Computer Science Department and I will have Rosanne Vrugtman as my technical advisor. My project will be a capstone project which will be worked on independently as part of the class CS 4991. My project goal will be to explain how machine learning models have their information leaked, describe the state-of-the-art techniques that prevent data leaks, and how the topic can be incorporated into CS 4774 Machine Learning. There are no unusual constraints and the methods used will be just research. If my project succeeds in its goals, students who take Machine Learning will understand the privacy issues machine learning models face and prevent data leaks in their machine learning models.

Front End Protection: How the GDPR Is Enforced

How do social groups in the European Union enforce General Data Protection Regulation compliance?

How can user information be protected? The European Union (EU) grappled with the evolution of the right to privacy in the internet age. From 2002 onwards the EU has provided guidelines to individual nations to regulate private information usage (Vanberg, 2021). Nevertheless, large corporations were able to maintain non-compliant data collection schemes through the lack of regulation for the entire EU (Vanberg, 2021). In 2018, the EU

adopted the General Data Protection Regulation (GDPR) which provided large financial penalties to corporations that collected data on EU citizens independent of the corporation's location (Holbl 2021). With the adoption of the new data regulation, how did advocacy groups enforce GDPR compliance?

The participants in the enforcement of the GDPR can be split into 3 groups: government bodies, advocacy groups, and industry bodies. The GDPR has divided the responsibility of enforcement of the GDPR into a federation-level board called the European Data Protection Board, and state-level Data Protection Authorities (Burgess, 2022). Individual Data Protection Authorities investigate how companies in their country break their laws and set fines for the companies' unlawful behavior (Beesley, 2021). However, if the decision is not agreed upon, the One-Stop-Shop portion of the GDPR requires the European Data Protection Board to mediate the number of fines given to the offending corporation (Burgess, 2022). There are disagreements on how effective the federalized nature of GDPR enforcement with Helen Dixon, Data Protection Commissioner for Ireland, arguing that she "would classify the DPC as being very effective in the first four years of application of the GDPR," while Marie-Laure Denis, the head of French regulator CNIL, stated that "We still believe in the GDPR enforcement mechanism, but we need to make it work better—and quicker" (Burgess, 2022).

Advocacies have promoted the GDPR in diverse ways. NOYB is a legal advocacy that helps DPCs investigate large corporations (O'Faolain, 2022) and sues corporations for breaking the GDPR (Hamilton, 2020). In its public project summary, NOYB described its mission to "make privacy a reality" by closing the "huge gap between privacy protections on paper and in real life" (NOYB, 2017). Proton is a company that created GDPR.eu which provides information about the GDPR for small and medium-sized local business owners

(Wolford, 2019). Ben Wolford, a writer for Proton, argues that "inadequate understanding of the law remains the greatest obstacle to compliance for small- and medium-sized businesses" (Wolford, 2019). Finally, country-level organizations like the Irish Council for Civil Liberties improve enforcement of the GDPR by becoming a watchdog of their country's Data Protection Authority. The Irish Council for Civil Liberties has filed complaints against the Data Protection Commission for its failure to investigate Google's use of Real-Time Bidding (Qureshi, 2022), and written letters to the Irish Parliament and Senate to investigate Ireland's enforcement of the GDPR (Ryan, 2022).

Industry bodies have criticized the GDPR for its impact economically. Hazel Grant, head of the privacy, security, and information group at the law firm Fieldfisher, stated that "More and more businesses have allocated significant budgets to doing data protection compliance" (Burgess, 2022). Because of the expense of data protection compliance, apps on the Google Play store dropped by a third. According to researchers at the National Bureau of Economic Research, the privacy benefits of the GDPR "come at substantial costs in foregone innovation" (Janßen et al., 2022).

Researchers have investigated how successful the GDPR is at improving privacy. For example, Holbl (2021) found that the decentralized nature of the EU allows for inconsistent enforcement of the GDPR from country to country, while Tsohou et al (2020) conclude that the lack of awareness is a larger issue in the enforcement of GDPR. Finally, Vanberg highlights how the conception of the right to privacy through EU regulations limit the ability to protect user information..

References

Beesley, A. (2021, September 2). Record €225m fine imposed on WhatsApp by Irish regulator for 'severe' breaches of privacy law. *The Irish Times.* https://www.irishtimes.com/business/technology/record-225m-fine-imposed-on-whatsapp-by-irish-regulator-for-severe-breaches-of-privacy-law-1.4663042

Burgess, M. (2022, May 23). How GDPR Is Failing. *Wired.* https://www.wired.com/story/gdpr-2022/

Hamilton, I. A. (2020, November 16). Apple illegally tracks iPhone users to target them with ads, EU privacy activism group claims in lawsuit. *Business Insider*. https://www.businessinsider.com/apple-iphone-privacy-illegal-tracking-cookies-eu-lawsuit-advertising-2020-11

Holbl, M., Kezmah, B., & Kompara, M. (2021). Data Protection Heterogeneity in the European Union. *Applied Sciences-Basel*, *11*(22), 10912. https://doi.org/10.3390/app112210912

IBM. (2022, October 19). Cost of a data breach 2022. https://www.ibm.com/reports/data-breach

ICouldBeStoned2Death. (2015, July 23). I May Get Stoned to Death for Gay Sex (Gay Man from Saudi Arabia Who Used Ashley Madison for Hookups) [Reddit Post]. R/Lgbt.

www.reddit.com/r/lgbt/comments/3ebzzj/i_may_get_stoned_to_death_for_gay_sex_gay_man/

Janßen, R., Kesler, R., Kummer, M. E., & Waldfogel, J. (2022). GDPR and the Lost Generation of Innovative Apps (Working Paper No. 30028). *National Bureau of Economic Research.* https://doi.org/10.3386/w30028

NOYB (2017). Making Privacy a Reality. https://noyb.eu/sites/default/files/2020-03/concept_noyb_public.pdf

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. *2008 IEEE Symposium on Security and Privacy (Sp 2008)*, 111–125. https://doi.org/10.1109/SP.2008.33

O'Faolain, A. (2022, March 14). High Court challenge brought against DPC over processing of personal data. *The Irish Times*. https://www.irishtimes.com/business/technology/high-court-challenge-brought-against-dpc-over-processing-of-personal-data-1.4826689

Qureshi, S. (2022, March 16). Irish civil liberties group sues DPC over failure to act on massive Google data breach. *JURIST Legal News & Commentary*. https://www.jurist.org/news/2022/03/irish-civil-liberties-group-sues-dpc-over-failure-to-act-on-massive-google-data-breach/

Ryan, J. (2022, September 27). DPC problems are not due to Irish legislation, ICCL tells EU Parliament LIBE Committee & Oireachtas Justice Committee. Irish Council for Civil Liberties. https://www.iccl.ie/news/dpc-problems-law-data/

Thielman, S. (2015, August 19). Top data security expert fears traumatic aftermath in Ashley Madison hack. *The Guardian*. https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hack-outcome

Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., & Crespo, B. G.-N. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. *Information and Computer Security*, *28*(4), 531–553. https://doi.org/10.1108/ICS-01-2020-0002

Vanberg, A. D. (2021). Informational privacy post GDPR - end of the road or the start of a long journey? *International Journal of Human Rights*, *25*(1), 52–78. https://doi.org/10.1080/13642987.2020.1789109

Wolford, Ben (2019). Proton Mail created GDPR.eu, to help businesses achieve GDPR compliance. https://proton.me/blog/gdpr-compliance-guide

Zanella-Béguelin, S., Wutschitz, L., Tople, S., Ruehle, V., Paverd, A., Ohrimenko, O., Köpf, B., & Brockschmidt, M. (2020, November). Analyzing Information Leakage of Updates to Natural Language Models. *ACM Conference on Computer and Communication Security (CCS)*. https://www.microsoft.com/en-us/research/publication/analyzing-information-leakage-of-updates-to-natural-language-models/