Research Statement

Ron Hirschprung Ph.D.

Department of Software and Information System Engineering
Faculty of Engineering Sciences
Ben-Gurion University
hrony@post.bgu.ac.il

1. Synopsis

The digital era introduces significant privacy issues (risks and fairness) which are mainly ~~an~~the ~~outcome~~ result ~~a~~the machines' computational power, and. ~~The~~ users ~~is unable~~ are no longer able to manage ~~the~~ their online privacy effectively~~by himself~~. My research interests ~~are at~~ focus on ~~the adoption of~~using machines ~~by~~ to implement~~ing~~ AI-based algorithms to mitigate and ~~to~~ control th~~e~~ose issues. I plan to establish a research group that will develop methodologies and technologies to ~~carry out~~: a) carry out some transformations on published datasets in order to minimize privacy risks by increasing anonymization, while maximizing the relevancy of the dataset to its designated purpose; b) develop~~ment of~~ a proxy server that isolate data analyzer the data itself; c) provid~~e~~~~ing~~ an automated mechanism to ~~tune~~ balance the trade-offs between utility and privacy cost (after it has been optimized by the transformations), so that a user can still elicit his/her preferences to the technologically compl~~ex~~~~icated~~ environment. These advanced methodologies should address both the requirements of legislators / regulators and the demand for 'trust' which is a viability feature for many IT systems.

2. The Trade-~~O~~off between Utility and Privacy-Loss in the Digital Era

An inherent trade-off between the utility ~~that is~~ provided by Information Systems (IS), and the cost of privacy is a growing problem, and in the current digital era ~~empowered to a level that~~ may even threatened the process of further adoption of those systems. The increase of data collection ~~means~~technologies, the feasibility (mainly economic~~ally~~) of mass storage,

Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted
Comment [A1]: Perhaps you can
Formatted
Formatted
Formatted
Formatted
Comment [A2]: Please clarify the
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Comment [A3]: Do you mean: the
Formatted
Formatted
Formatted
Formatted
Formatted

and the availability of computational power (e.g. discovering ~~some~~ "hidden" facts about an individual by implementing machine learning) – yield a growing awareness, and also~~thus~~ concerns regarding privacy issues. The phenomena can be demonstrated in a variety of domains. One of them may be A*utomated Decision Making*, by implementing AI-based algorithms. In this case, an agent ~~that acts~~acting on behalf of the user, or as a service of another entity, requires a significant amount of information about the user in order to carry out its tasks. The agent's function yields decisions from ~~a~~ given information, however, when many decisions are given the function might be reversed yielding the source information.

Another important application domain is *Medical Informatics*~~—~~ where currently ~~a~~ clinical data of relatively large groups of patients is analyzed and can yield significant findings. Even though~~Also~~ key attributes are omitted from the dataset (anonymization), the individual can sometimes still be identified by the quasi identifiers or ~~even~~ by other ~~the~~ sensitive data. Legislators are aware of the risks of privacy violation ~~risk~~, which are related ~~perceived as~~to human rights, and make research difficult.~~—~~ In this case the trade-off is stretched radically since on one side of the scale lies a lifesaving factor and on the other side a disclosure of maybe the most sensitive information ~~that an~~ an individual ~~hold~~ possesses.

A common approach to handle~~ing this type of~~such trade-offs, is to provide the user with a mechanism that enables its' regulation~~ng~~, e.g. by configuring the system. This task however, as simply~~e~~ as it may seem~~, to be,~~ holds some difficulties which actually prevent its implementation. First, the complexity of the~~o~~se sophisticated systems, not to mention the~~its~~ indirect privacy violation ~~effect~~ is beyond the literacy of the layman user. Second, users may be prone ~~incline~~ to cognitive laziness thus avoiding such tasks. And finally, user behavior is characterisized~~tic~~ by risk aversion and not by maximizing expectancy. The direct outcome of the~~o~~se insights is that a human being cannot handle privacy issues that are introduced by machines, and machines must be harnessed to successfully carry out this task. In My research~~es~~ I~~'m~~ intend to develop algorithms based mainly on mathematical models that will provide a solution to these~~is~~ trade-offs at two levels~~in two layers~~: a) by *Mitigating the trade-off*. b) by *Controlling the trade-off*. The above mentioned methodologies ~~are applicable at~~employ the PbD (Privacy by Design) approach, as required by regulators (e.g. GDPR).

3. Mitigating ~~the~~ Privacy Loss

Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted

A published dataset, even when anonymized can still be a source for privacy disclosure. However, given the (legitimate) purpose of publication of the dataset ~~publication~~, it has been shown that by applying some transformations to the data, e.g. data perturbation, the purpose can still be served and~~but~~ privacy risks ~~are~~ reduced. My research ~~mission~~ goal here ~~in this section~~ is to find and define th~~e~~ose transformations as AI machine learning agents that can be applied on-line (as required in contemporary information systems). I distinguish two levels of protections: a) against inference attacks that rely~~ies~~ on aggregated data published from the dataset; b) against inference attacks that rely~~ies also~~ on auxiliary information ~~that~~ which cannot be controlled by the defender. The transformation can be implemented on~~in~~ a proxy server for example, and an authorized administrator should have the ability to set boundaries to the privacy disclosure risks while under those constrains the published dataset is optimized to provide maximal purpose achieving efficiency.

~~In~~ At an advanced phase of this research project, we intend to develop ~~seek for~~ a novel methodology ~~to~~ for applying Machine Learning on Hidden Data (~~I called it for now:~~ ML-HD). The concept is to create a research development methodology ~~of researches~~ based only on conveying logic to a proxy without access to the raw data. This methodology which belongs to the ~~circle~~ category of PETs solutions (Privacy-Enhancing Technologies) has~~ve~~ great advantages over existing methods such as Obfuscation. This way, machines can for example provide ~~a~~ personal data-mining to an individual without ~~a~~ significant risk of data disclosure.

These models can be tested empirically ~~be tested~~ by sampling real data and applying both ~~both to the original dataset and the sanitized dataset~~: a) inference attacks to measure the amount of privacy disclosure reduction; and b) processing the data for providing the purpose to measure the amount of efficiency loss, to the original dataset and the sanitized dataset.

4. Controlling Privacy

This layer of privacy protection should be implemented as a second phase ~~after~~ once the trade-off ~~was~~ is optimized.~~, and~~ Its purpose is to enable the user to tune the trade-off according to personal preferences. In ~~M~~my previous research, I developed an algorithm to reduce the configuration space (that ~~may~~ can control this trade-off) and thus provid~~e~~ing the user with a more efficient ~~choice~~ architecture to elicit preferences. The algorithm was

Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold, Highlight
Formatted: Font: Bold, Complex Script Font: Bold, Highlight
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted: Font: Bold, Complex Script Font: Bold
Formatted
Formatted
Comment [A4]: Please clarify this
Formatted
Comment [A5]: Is this what you
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted

empirically tested on Facebook real data (n= 266 users ; 21,950 posts), ~~proofed~~ and ~~to~~ provided a significantly better ~~choice~~ architecture than current Facebook's defaults. By adopting a different approach, we developed a methodology to quantify the value of privacy in terms of intrinsic value~~d~~ (e.g. Dollars). By doing so, it is also possible to accommodate ~~also~~ average utilities and social fairness in the objective function.

The ability to quantify privacy loss provides~~open~~ opportunities **for a wide range of implementations that can automatically configure digital systems on behalf of a user. I am interested in developing methodologies to establish Intelligent-Agents (IA) that will carry out this mission. The IA should have the ability to respond to the dynamic changes both of the environment and of the user's preferences.** Intuitively~~I~~, it seems that the IA design is domain oriented, ~~H~~however I seek **to generalize the problem as a step towards creating a universal data disclosure tuning IA.**

Formatted: Font: Bold, Complex Script Font: Bold

Formatted: Font: Bold, Complex Script Font: Bold

Formatted: Font: Bold, Complex Script Font: Bold

Formatted: Font: Bold, Complex Script Font: Bold

Formatted: Font: Bold, Complex Script Font: Bold