MIND YOUR DATA

YOUR GUIDE TO REGAIN PRIVACY & CONTROL!

Written by:
MSc. Information System students at Vienna University of Business and Economics

WU
WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

Brussels, January 2018

Dear Reader,
This brochure contains a noteworthy benchmark on the data-handling practices of 2017's major online services and their smaller, but privacy-friendly competitors. As we can learn from a group of Austrian business informatics students, some young and ambitious companies offer us not only e-mail, messaging, calendar and location apps in a convenient and free way, but they do so without infringing too much our privacy. They are open and transparent in their efforts to provide services, give users choices and help to mitigate data-power asymmetries. They do so, while not scoring poorly when it comes to service convenience. This is good news!

I appreciate the students' effort to give these 'good' companies a forum, because **I was rapporteur of the General Data Protection Regulation (GDPR) in the European Parliament.** One important claim of this legislative effort has been that citizens value privacy and that companies, which offer it, can gain a competitive edge. This student work demonstrates the ethical consciousness of an educated generation, which is becoming aware of the personal data abuses happening in the online world today. Most importantly, it shows how young companies make a difference in their privacy practices and therefore receive higher ratings.

The new EU legal framework for the protection of personal data is already becoming a global standard as many companies set it as their general standard even for services and businesses outside of the EU market. We can see how the subject of data protection serves as an example how effective regulation in a digital market and society can still work in light of high connectivity and cross-border activities.

I hope that efforts like this will help to inspire the online service market to improve their privacy proposition and I also want to encourage citizens to continue a bottom-up engagement of this type to raise privacy awareness among the general public.

Kind regards,
Jan Philipp Albrecht
Member of the Europen Parliament

Vienna, January 2018

Dear Reader,
For a long time, universities have been the place where critical thinking has taken place; where our societies' practices were critically reflected; where the ethics of the present time were hotly debated and hence, where thinking advanced. This thought leadership role of the universities was even more crucial than the churning out of technical innovations. And it is in this role that universities have served as nourishers of society at large. The debates and thoughts pursued at the "ivory tower" have for centuries trickled down into the public mind.

Correspondingly, I perceive it as my duty to not only teach my students at WU on the subject matter of Privacy and Security as part of their education in Business Informatics, but also to promote critical reflection on what they learn. And I want to give them a purpose. This brochure is the result of this process. Our WS 2017 class on "Privacy & Security" has led to the analysis found in this brochure: a critical reflection on the privacy practices of today's leading players in the field of social media, messaging, map and calendar, as well as e-mail services. As the readers of this piece will immediately recognize, our market leaders are no 'white sheep'. Indeed, they compare poorly to their younger competitors, who embrace the importance of personal data protection and promise to rebalance the power of the people in the digital world.

This brochure should not be understood as a piece of 'scientific' research, nor is it possible to live up to the standards of an entity such as "Stiftung Warentest" that is able to invest months of research and abundances of money on product quality tests. Rather, it should be understood as a critical investigation of practices by business informatics students who have taken care to inform their co-citizens of practices in the online world compromising our privacy today. It is a piece dedicated from 'citizen-to-citizen'; potentially from 'young-to-old'; from 'university-to-public'. I hope you readers can appreciate this effort.

Kind regards,
Prof. Dr. Sarah Spiekermann
Institute for MIS at WU Wienna; Idea & Mentorship

IN A **NUTSHELL**

We live, share, buy, sell, communicate and play in a digital world, where everything we do leaves a digital trail: sending an instant message or email to friends or colleagues; syncing our contacts, calendars, photos with our cloud accounts; sharing interests, opinions, photos, whereabouts on social media; searching for and purchasing products in online shops... the list goes on and on. We save our passwords for later use ('how convenient' we think while we click the "save my password" button) and we use a social media profile to sign up for dozens of other services (again, convenient!), not realizing that our actions on the Internet are accumulating into huge compilations of our behavioural history.

Corporate actors have found an opportunity to capitalize on this wealth of information, an unprecedented chance to understand their customers like never before, and have been engaging in unrestricted digital monitoring and data analysis. This relationship companies have with customers can be compared to a game of poker, where one of the players has his hand open and the other keeps his cards close.

"So, what's the problem?", you might be asking yourself. In this brief introduction, we aim to summarize how exactly, by using email, messenger services, social networks, online calendars, and navigational map services, you are forfeiting control over your personal identity and private information. Throughout this brochure, you will find a set of criteria used to determine the privacy and integrity of a variety of service applications. The failure of companies to meet these standards represents an abuse of power without consent, an inconsiderate position on the individual's right to privacy and/or anonymity. As such, where grades for a particular criterion are poor, the respective aspect of privacy control is threatened.

Antje Schwarz
Editor in Chief

Bojana Trajkovska
Design & Layout

Luada Toro
Design & Layout

PROTECT
YOUR DATA,
PROTECT
YOURSELF!

CONTENT

* Please note that this work is written by students as part of a course. WU, nor the students, nor the Privacy & Sustainable Computing Lab are liable for this material.

Perhaps you've picked up this brochure because you're eager to explore how you might regain some control over your data. Perhaps, instead, you're reading because you're doubting that you've even given up control over any of your data, yet curious none the less about what we might have to say. This brochure represents an opportunity for everyone (no technical expertise needed!) to increase awareness for how everyday user behaviours or patterns might be exposing personal, private information to corporates and hackers alike, to inform on risks around sharing and transferring data, and to instill a mindset amongst a wider audience that is cautious of data privacy threats and aware of how to avoid them. Let us introduce you to five services that put your privacy at more risk than you might have suspected, share with you the risks involved in using these services, and offer actionable next steps in the form of advice and app alternatives to regain control over YOUR data and YOUR privacy.

ABOUT US

We are a group of MSc. Information Systems students at Vienna University of Business and Economics (WU), taking a class in Data Privacy & Security as part of the Institute for Management Information Systems. Many of us were unaware of how our online behavioural patterns are shaping our consumer profiles and/or exposing us to various privacy risks. Conducting an evaluation using a pre-defined list of privacy criteria, we considered to what extent many of today's most-used internet and smartphone applications are placing user privacy at the heart of their value proposition, and felt it was important to offer up these findings to you through this brochure. This project was conducted in collaboration with Privacy & Sustainable Computing Lab at Vienna University of Business and Economics.

CRITERIA TO BENCHMARK **ONLINE SERVICES**

In the following pages, we - the Privacy & Security Class of WS 2017 (at WU Vienna) - seek to define and explain the criteria we used to compare, rate and benchmark service provider offerings for each of five service categories (messenger, social media, location-based/maps, calendar, and email services).

In total, seven criteria were deemed essential factors in deciding whether an application constitutes a privacy-friendly service: information control, decision control, decision control for audiences, behavioural control, technology paternalism, privacy-by-design, privacy friendly defaults. In addition we judged on the service appeal, because often privacy is deemed to come at the cost of convenience or usability.

It should be stated clearly that ratings for each of these criteria exemplify our personal opinions and views. We have taken great care to support our opinions with clear reasoning logic and, where appropriate, facts. This reasoning has been documented and can be found in the appendix of this brochure.

INFORMATIONAL CONTROL

Information control is a criterion used to evaluate the extent to which users are informed about data processing activities of the service provider. In assessing the information control provided from an application, we consider, amongst other factors, whether the information provided by the service provider on its data activities is meaningful. In other words, whether all provided information from the service provider is easy to understand from a user perspective, whether it is presented clearly and concisely in plain language. Also critical to meet "meaningful information" standards is the notion of completeness: has a service provider revealed fully all data processing activities application users are subject to? This includes data collection, aggregation, analysis, and dissemination activities. Data dissemination is the service provider's act of sharing or selling user data to third parties, often outside of the context of the service provision. In conclusion, the information control grade for each application evaluated represent the service provider's overall efforts to fully and truthfully inform the users about data handling practices.

DECISIONAL CONTROL

Decision control is a criterion used to evaluate the extent to which users are given a choice over data processing activities conducted by the service provider. When assessing the decision control of an application, we take into consideration, for example, whether the decision to share or sell user data can be made freely and voluntarily by the user. By definition this condition excludes any service provider implementing "service coupling", whereby a take-it-or-leave-it situation is the result of the inability to deny data processing whilst still benefiting from the service. This criterion therefore takes into account whether the user is provided with the choice to decline data processing activities of the service provider without penalty. Additionally, we consider whether the data-sharing decision options are easily found on the website or within the application, not hidden under layers or in obscure locations impossible to find, and whether these options are opt-in by default, requiring a user to manually and actively agree to the sharing of their data, or opt-out, where a user must undergo effort to ensure privacy. In conclusion, decision control ratings represent the overall effort undergone by the service provider to provide users with choices concerning data handling practices.

DECISIONAL CONTROL FOR AUDIENCE

Decision control for the audience is a sub-criterion of decision control dimension explained above, focusing specifically on decisional control over choosing who to share personal data with. Indeed, this criterion is used to evaluate whether users are given a choice in determining the audience for their posts, whether the users can decide who will and who will not be able to access and view their posts. Decision control criteria for the audience is especially important for social media applications as it enables the user to have additional privacy options and is used to distinguish between different social media channels (e.g. Facebook offers the user the possibility to decide who from their friends will be able to see a specific post, whereas Instagram does not provide this option). In conclusion, the decision control for audience rating for each application represents the overall effort made by the service provider to provide users with choices over personal data sharing to specific audiences, with a focus on content access limitation.

BEHAVIOURAL CONTROL

Behavioural control is a criterion used to evaluate the extent to which users are provided with feedback that their decisions regarding the allowance or denial of data processing activities by the service provider have been respected and implemented. While evaluating behavioural control of an application, we consider whether the users are in the first place given the choice to accept or deny particular processing activities, but also whether these choices may be revoked or changed at any time via easy-to-comprehend and accessible mechanisms, for example using tick-boxes within an easy-to-locate menu. One particular observation is that applications often do not respect that choices made by users are absolute, and instead harass users with pop-ups asking for or suggesting consent to data collection. Another dimension taken into consideration is the question of whether the service provider provides a contact point (email address, phone number, or similar) through which the user are able to verify the respectful treatment of their privacy choices. In conclusion, the behavioural control rating of each application represents the overall effort made by the service provider to grant users feedback on updates to data handling practices to mirror user choices.

TECHNOLOGY PATERNALISM

Technology paternalism is a criterion used to evaluate the extent to which a service is patronizing the user, meaning it executes autonomous actions that interfere with the user's freedom. Where paternalism is present, the service does not offer the user an option to override these actions. Several dimensions are taken into account within this criterion, for example whether the service is sending unsolicited messages (e.g. push-messages that appear on screen while the user is actively using the application) or the existence of display ads that the user is forced to view/watch (e.g. Facebook ads that appear on the user's feed). A further dimension addresses the customization aspect, in particular, the option for the user to configure his/her own interface/screen (e.g. reconfiguring/ moving different buttons, blocks of content and design/style of the interface). Furthermore, a paternalistic service is considered one that is using demand-style language (e.g. words and phrases such as "must"; "to-do"). The last dimension addresses the paternalistic functions that may be implemented within the service itself (e.g. calendars automatically adding events for flights based on booking confirmation e-mails). In conclusion, paternalism rating for each application represents the overall effort made by the service provider to grant users freedom in their actions and control over their usage of the application without patronizing "suggestions" from the service provider.

PRIVACY BY DESIGN

The criterion of privacy-by-design analyzes whether the service provider has designed the application/service in a way that the data does not need protection, because the "channels" for data transfer are, from initial design stages, designed in a way that preserves the privacy of the user. One dimension of privacy-by-design is whether the service provides encryption of data transfers (e.g. the messages exchanged between users of a messaging application are not accessible from anyone except them). A further dimension addresses the architecture design of the service, in particular, whether the application has a decentralized architecture (e.g. is the communication between the users in a messaging application running through the provider's architecture or via peer-to-peer architecture). The possibility to use the application without authenticating yourself is the last dimension considered, meaning that an application is conforming to the privacy-by-design criterion if and when the user has the option to use the application anonymously. In conclusion, the privacy-by-design rating for each application represents the overall effort made by the service provider in the engineering process to value and safeguard the privacy of its users.

PRIVACY FRIENDLY DEFAULTS

Privacy friendly defaults is a criterion used to evaluate the extent to which the applications' default settings are privacy-preserving. "Default" is referring to the states of different options in an application at the time of download, before a user has changed or manipulated any of its settings. The first dimension under this criterion is "data-minimization", in order words the extent to which the service provider collects and processes only the information required to offer the service and nothing more. Is the service provider processing the user's data only for the service delivery or does it collect data beyond this purpose? (e.g. is the user's e-mail requested on the social media platforms used only for registration purposes or also for third-party advertisements) The second aspect of privacy friendly defaults is considering whether the service provider exposes the user to unnecessary openness (e.g. is the navigation application requiring access only to the user's location or also to his/her camera and microphone). In conclusion, the privacy friendly defaults rating for each application represents the overall effort made by the service provider to preserve the privacy of the users without requiring them to reconfigure the settings of the application.

SERVICE APPEAL

Service appeal is a criterion used to evaluate the extent to which the users have a pleasant experience while using the application. This criterion is addressing the design of the application, drawing on four dimension sub-criteria. The first focuses on the appearance of the interface and whether it is aesthetically "inviting" to use. This encompasses the style of the objects, the color palette used, the arrangement of different components (e.g. an application with too many elements and unbecoming color combinations might be considered not to have an aesthetically pleasing interface). Further, the easy-to-use dimension is assessed in terms of personal experience. The intuitive design of the application that does not require the user to gain some additional knowledge to use the application contributes to this dimension. (e.g. having the BACK button placed on the left upper side of the interface like on the majority of applications; in this case the user does not need to acquire new knowledge for this simple task). The possibility for an easy configuration is another dimension which can be seen as a "back-up". In case the user does not find the application easy-to-use by default, the service appeal would increase if the provider offers the possibility to the user to move around the contents and elements of the interface so that they match his/her expectations. In conclusion, the service appeal rating of each application represents the overall effort made by the service provider to offer the users with an easy-to-use and appealing interface and experience.

PRIVACY IN MESSENGER APPS

RESEARCHED BY **CHRISTIAN & YOAN**

Increasingly, more and more people express concerns regarding social media platforms collecting user data for purposes apart from the actual service. But few people recognize that the same is true for messaging. In many forums, people write about excessive uploading data caused by their mobile messaging apps. For instance, in May 2017, user Pratt07 reported on the "Best for Android"-Forum about Facebook's Messenger uploading nearly 4GB of background data in one single night (while only around 3 MB of foreground data was consumed within the days before by himself). The month before, Pratt07's Messenger uploaded unbelievable 11GB of data. Consequently, Pratt07 was faced with a $600 bill from his telecommunications provider. What's more, Pratt07 is not the only one to report about such messaging apps behaviours – and indeed, Facebook's Messenger is not the only messenger service mysteriously gathering and transmitting data. One big question remains: What kind of data is transmitted? Even if it were the total sum of all conversations within a respective messenger, this wouldn't be much more than a few MBs.

	MESSINGER	WHATSAPP	VIBER	SIGNAL	WICKR ME
INFORMATIONAL CONTROL	⬜🟥⬜⬜⬜⬜⬜	⬜🟥⬜⬜⬜⬜⬜	⬜⬜🟧⬜⬜⬜⬜	⬜⬜⬜⬜⬜⬜🟩	⬜⬜⬜⬜⬜🟩⬜
DECISIONAL CONTROL	⬜⬜🟧⬜⬜⬜⬜	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜⬜🟩⬜⬜	⬜⬜⬜⬜⬜🟩⬜	⬜⬜⬜⬜⬜⬜🟩
BEHAVIORAL CONTROL	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜⬜🟩⬜⬜	⬜⬜⬜⬜🟩⬜⬜	⬜⬜⬜⬜🟩⬜⬜	⬜⬜⬜⬜🟩⬜⬜
PRIVACY FRIENDLY DEFAULTS	⬜⬜🟧⬜⬜⬜⬜	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜⬜⬜🟩⬜	⬜⬜⬜⬜⬜⬜🟩
TECHNOLOGY PATERNALISM	⬜⬜⬜🟨⬜⬜⬜	⬜⬜🟧⬜⬜⬜⬜	⬜⬜⬜⬜🟩⬜⬜	⬜⬜⬜⬜⬜🟩⬜	⬜⬜⬜⬜⬜🟩⬜
PRIVACY BY DESIGN	⬜🟥⬜⬜⬜⬜⬜	⬜⬜🟧⬜⬜⬜⬜	⬜⬜🟧⬜⬜⬜⬜	⬜⬜🟧⬜⬜⬜⬜	⬜⬜⬜⬜🟩⬜⬜
SERVICE APPEAL	⬜⬜⬜⬜⬜🟩⬜	⬜⬜⬜⬜⬜🟩⬜	⬜⬜⬜⬜⬜⬜🟩	⬜⬜⬜⬜⬜🟩⬜	⬜⬜⬜⬜⬜🟩⬜

*Each bar, left to the right, represents a grade starting from very poor, poor, fair, neutral, good, very good, excellent.

MESSENGER APPS - RISKS

Mobile messaging apps very popularly complement smartphones, expanding their use beyond simple SMS or telephone communication by offering additional functionality via constant and instant communication in the form of texts, voice notes, video clips and photo sharing, and even calling. Their popularity is based not surprisingly on their convenience. However, these can unfortunately pose risks to a device owner's privacy unless certain measures are taken. There are several potential privacy risks to users involved in the use of messaging applications. Your messages can be spied on or even scanned. Depending on the type of encryption offered by the messenger provider, meta data may still be collected. This means that although a provider is not able to read your messages, they are still able to identify that you sent photos and messages to certain people in a certain country, and so forth. Because of this, a messenger service offering end-to-end encryption such as WhatsApp might still be intruding on your privacy. But what really makes messaging app use risky is that users have to trust the app developers with their personal information, as messaging apps require users to sign up prior to their use (for example, WhatsApp requires your phone number to set up your profile). Because of the apps' popularity, messaging services have also become a huge target for data server attacks that can lead to a data breach and personal data leakage. The more popular messaging apps become, the more they come under attack!

YOUR POTENTIAL ACTION STEPS?

FIRST STEPS

• As most of the messengers are delivered with lowest possible privacy defaults, it is recommended to set the smartphone privacy settings in advance (e.g. block access to locations, contact lists, etc). Furthermore, be careful what you send to others (especially in terms of photos) - communication partners are always able to take screenshots of your messages. Exhaust in-app privacy settings. As they are usually easy to find, quickly browse through them and be rather too closed than too open (in terms of access to your smartphone-device and software)

• Although all instant messengers need to have a big user-base to exploit their network-effects, try to convince your social environment to use alternative messaging apps (such as Signal and Wickr Me);

• Most modern messengers provide encryption for messaging and calls. Use encryption if you want to mitigate risks in case your data is stolen;

• Use privacy friendly messengers this will encourage the big players to work towards becoming more privacy

FOR ENTHUSIASTS

Here are some further tips for those who want to be 100% secure.

• Always use end-to-end encryption as it is still by far the strongest measure of an app's security. But there's plenty to consider, from permissions to open-source code. Remember, any app that makes lofty promises should be investigated. Security is hard, and user vigilance is key. All the apps we tested provide end-to-end encryption – in terms of Facebook's Messenger, only "secret conversation" mode is end-to-end encrypted

• Use VPN: Using a VPN is the most basic way to secure all of your traffic. Once you connect to a VPN, your traffic is encrypted so no one snooping can see what you're looking at. This is particularly useful when you're on public networks where you might not control your internet connection. If you want to create your own VPN, visit, for instance, chose one from https://thatoneprivacysite.net/vpn-section/

PRIVACY IN SOCIAL NETWORK APPS

RESEARCHED BY **RUONAN & ENSAR**

In 2015, Formula One driver Jenson Button had his house robbed in St. Tropez, France. Button and his wife, Jessica Michibata, were staying in a rented holiday villa, which thieves broke into and cleaned out, taking amongst all things, Michibata's $388,000 worth wedding ring. The robbers knew exactly where Button and Michibata were, because of Michibata's posts on Instagram that night. They used her posts as a signal for when they should strike. Similarly, reality TV star and socialite Kim Kardashian publically fell victim to a robbery in Paris that resulted in damages of over 10 million euros after revealing on social media that she will be traveling, showing off her jewellery. "The jewels were shown on the Internet, and [she said] that she didn't wear fakes. The time she would arrive in France, you just had to look at the Internet and you knew everything, absolutely everything," said the implicated 60-year-old veteran robber and leader of the group that robbed Kim Kardashian in a police report.

	FACEBOOK	TWITTER	INSTAGRAM	DIASPORA	ELLO
INFORMATIONAL CONTROL	□□□□□🟩□	□□□🟨□□□	□□□🟨□□□	□□□□□□🟩	□□□□□🟩□
DECISIONAL CONTROL FOR COLLECTION OF PERSONAL DATA	□□🟧□□□□	🟥□□□□□□	🟥□□□□□□	□□□□□□🟩	□□□□□□🟩
DECISIONAL CONTROL FOR AUDIENCE	□□□□□□🟩	□□🟧□□□□	□□🟧□□□□	□□□□□□🟩	🟥□□□□□□
PRIVACY FRIENDLY DEFAULTS	□□🟧□□□□	🟥□□□□□□	🟥□□□□□□	□□□□□□🟩	□□□□□🟩□
TECHNOLOGY PATERNALISM	□□□□🟩□□	□🟧□□□□□	□🟧□□□□□	□□□□□□🟩	□□□□□□🟩
PRIVACY BY DESIGN	□🟧□□□□□	□□🟧□□□□	□□🟧□□□□	□□□□□□🟩	□🟧□□□□□
SERVICE APPEAL	□□□□□□🟩	□□□□□□🟩	□□□□□□🟩	□□□🟨□□□	□□□□🟩□□

*Each bar, left to the right, represents a grade starting from very poor, poor, fair, neutral, good, very good, excellent.

SOCIAL NETWORK APPS - RISKS

Social networks are one of the most widely used services on the Internet today. They offer platforms on which people can connect with peers, friends, and family all around the world, sharing photos, videos, links, events, to name a few. On the other hand, they embody many risks that could potentially endanger you or threaten your privacy. Social network profiles, with photos, activities, opinions, and networks or connections, are "online versions" of us, mirroring our behaviours and even personalities. This inherently exposes you to identity theft. Take a minute to imagine what someone can do with access to your social network account: communicate with others as though he were you, pass on private information to others, harm your reputation, etc. Besides this, burglars, con artists and hackers hide behind fake accounts to easily get in touch with you and lead you into scams. Also, harmful to social network users on a platform is the ability for malicious apps and phishing scams to leverage the platform to reach out to you; one click on the malicious app or naively entering your personal data on the phishing link can expose you to an attack on your private information within seconds. While the aforementioned risks are perhaps the more daunting scenarios, there are many more risks to keep in mind that do not stem from malicious hackers or "criminals". The social network providers themselves are collecting personal and behavioural data from you. They are admitting to using and selling this data beyond service improvement purposes. Unfortunately, very few people are aware that the biggest social networks (Facebook, Twitter, Instagram, etc.) have essentially created business models around selling user data to third parties. Often used to tailor personalized ads at particular sub-groups of users, such data-selling practices pose critical privacy risks. Beyond personalized ads, they can render you victim to more severe consequences when your personal data is used to calculate your credit score, insurance fee, etc.

YOUR POTENTIAL ACTION **STEPS?**

FIRST STEPS

- Use security friendly apps we recommend (Diaspora and Ello)
- Think twice about accepting friend requests from people you don't know or who haven't been connected to you through legitimate, verifiable means
    - Read the profile carefully
    - Check out their friends & if you don't have good feeling about somebody, block the request
- Use high privacy control. Choose appropriate audience for your posts
- Select strong passwords, change passwords regularly and use different passwords for different platforms
- Pick a username that doesn't include too much personal information (if possible)
- Do not log into social networks on public devices. If you must, make sure to prohibit the browser "remembering" your password and always log out
- Be selective with posting and status updates (detailed personal information, location, time, etc.). Limit personal data you share in "biography" and "about me" sections
- Don't use Facebook account for creating accounts on other apps and services (Facebook "login")
- Secure posts you're tagged in – choose the appropriate audience for your friends' posts which include you
- Do not click on links or download apps that you are not familiar with

PRIVACY IN MAPS & NAVIGATION APPS

RESEARCHED BY NITA

Gilad Lotan, a data scientist, agreed to analyze a month's worth of two users' anonymized location data and create individual profiles for each one. Lotan did not know the users' identities. Data from both users was gathered via Google Maps Timeline web application, and sent to Lotan through a third person.
The users' location history helped to successfully build two profiles, by combining the location history data with other related online data. The first user was a 35-year-old male with a girlfriend but no kids who works in the film industry and travels a lot for work and on his own. The second user's home address was clearly identified. He works as an attorney at JB&P, owns a car, has a bank account with Wells Fargo and has kids. He likes hiking and cafes. The results did not only show the places both of these men visited, but also could easily tell their identity, their behaviours, traits and preferences.
In 2013, researchers from Massachusetts Institute of Technology and the Université Catholique de Louvain studied the location history data of 1.5 million users. They found that only four spatio-temporal points are required to uniquely identify 95% of the individuals whose data is collected and analyzed.

	GOOGLE MAPS	MAPS.ME	WAZE	HERE WEGO	OSMAND
INFORMATIONAL CONTROL	□□■□□□□	□■□□□□□	□□■□□□□	□□□□□□■	□□□□□□■
DECISIONAL CONTROL	□■□□□□□	□■□□□□□	■□□□□□□	□□□□■□□	□□□□□□■
BEHAVIORAL CONTROL	□■□□□□□	□■□□□□□	□■□□□□□	□□□□■□□	□□□□■□□
PRIVACY FRIENDLY DEFAULTS	■□□□□□□	□■□□□□□	■□□□□□□	□□□□□■□	□□□□□□■
TECHNOLOGY PATERNALISM	□□□□■□□	□□□□□■□	□□□□□□■	□□□□□□■	□□□□□□■
PRIVACY BY DESIGN	□□■□□□□	□□□□■□□	□■□□□□□	□□□□■□□	□□□□□■□
SERVICE APPEAL	□□□□□■□	□□■□□□□	□□□■□□□	□□□□□□■	□□□□■□□

*Each bar, left to the right, represents a grade starting from very poor, poor, fair, neutral, good, very good, excellent.

MAPS & NAVIGATION APPS - RISKS

Navigation maps offer a wide range of functionality to users when it comes to helping them reach a destination. It can be assumed that almost every mobile and desktop device has some navigation application installed and is used on a regular basis. That is the reason why it is important to know that there are serious risks attached to using them. These risks need serious attention and consideration. The story above shows how much personal and non-personal data one is sharing and giving away when using the navigation apps, and what information companies are extracting from this data (home address, work address, hobbies, preferences, behaviours, attitudes, traits etc.). This collected data is analyzed from companies. They use this analysis to create customer segments with the aim of targeting the right customers. This means that options (services and products) offered to users are limited based on what the users are most likely interested in, while hiding other offers. A lot of the location data collected is sold to interested companies. Credit reporting agencies are interested in knowing more about people and determine their credit score based on this data. Insurance companies might be interested in knowing the current and past locations of a client, as well as their driving style and driving patterns. Based on this information, the client is given respective car insurance rates. Users are wrong if they think these applications are free. Their data is the asset which is the most valuable to these companies.

YOUR POTENTIAL ACTION **STEPS?**

Navigation and maps applications are massively used because of the helpful services and added-value they offer. Suggestions provided here do not aim to encourage users to quit using applications or using them less. Instead, they offer guidelines on how to be more secure whilst using them, they advise you how to be more conscious and vigilant in interacting with the navigation and maps apps, be in control of the data being shared. Finally, users should feel that their data is shared voluntarily and with their consent.

BEFORE APP USAGE:

- Always read the Privacy Policy section of the navigation app: different applications define "in use" differently!
- Whenever starting to use the app, check the settings and make sure that the options are checked/unchecked as you prefer them to be
- If using the desktop-based version, always turn OFF cookies (if possible)

DURING APP USAGE:

- If the app offers location sharing with friends, remember to regularly check its state (in case the location sharing has been accidentally left active/turned with certain friends)
- If real-time traffic data is unnecessary, use offline maps, where possible, for navigation, and make sure that options regarding data collection are unchecked (turned OFF)

AFTER APP USAGE:

- Always keep your location services OFF. Turn ON only when needed (in your mobile and desktop devices);
- Always close navigation applications running on the background of a mobile device
- Do not automatically share location service data with navigation or any other apps
- If turning OFF cookies is not possible, never forget to delete them afterwards

PRIVACY IN CALENDAR APPS

RESEARCHED BY MARIE & BILYANA

A woman in a relationship shared her Google calendar with her boyfriend by granting his Google account access permission to her otherwise private calendar. Following their break-up, she removed his access rights to her calendar and changed her account password. Mysteriously, the ex-boyfriend began stalking her, following her to places he shouldn't have known she'd be. She contacted the police. It turned out that despite removing access rights to her calendar, the ex-boyfriend was still able to view her calendar entries. Turning to Google forums for help, she tried to resolve the access issue. It seemed that a password change and access removal had not sufficed in regaining her privacy. After trying everything suggested to her with no success, she set up a new Google account, still unknowing how her ex-boyfriend could read her calendar entries.

	GOOGLE	iCAL	OUTLOOK	SIMPLE	FRUUX
INFORMATIONAL CONTROL	⬜⬜🟧⬜⬜⬜⬜	⬜🟧⬜⬜⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜	⬜⬜⬜⬜⬜⬜🟩	⬜⬜⬜⬜⬜⬜🟩
DECISIONAL CONTROL	🟥⬜⬜⬜⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜	⬜⬜⬜⬜⬜⬜🟩	⬜⬜⬜⬜🟩⬜⬜
BEHAVIORAL CONTROL	🟥⬜⬜⬜⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜	⬜🟧⬜⬜⬜⬜⬜	⬜⬜⬜🟨⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜
PRIVACY FRIENDLY DEFAULTS	⬜🟧⬜⬜⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜	🟥⬜⬜⬜⬜⬜⬜	⬜⬜⬜⬜⬜⬜🟩	⬜⬜⬜⬜⬜⬜🟩
PRIVACY BY DESIGN	⬜🟧⬜⬜⬜⬜⬜	⬜⬜🟧⬜⬜⬜⬜	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜⬜⬜⬜🟩	⬜⬜🟧⬜⬜⬜⬜
SERVICE APPEAL	⬜⬜⬜⬜⬜⬜🟩	⬜⬜⬜⬜🟩⬜⬜	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜🟨⬜⬜⬜	⬜⬜⬜⬜🟩⬜⬜

*Each bar, left to the right, represents a grade starting from very poor, poor, fair, neutral, good, very good, excellent.

Risks associated with calendar applications for administrating your daily schedule are often overlooked and underestimated. Think of the nature of your calendar entries: they define where you will be (or won't be...), who you are with, where you are going and for how long, and sometimes include private notes not meant for the public eye.

CALENDAR APPS - RISKS

Particularly the use of online calendar applications opens doors of opportunity for privacy-invasive activity because of the need to store and transfer highly private organizational data on a remote server. While calendar services are convenient and easy to use, facilitating synchronization across multiple devices, calendar entries can be at risk. The synchronization of calendars across devices or even providers (you can, for example, sync Google's and Outlook's calendars) demands the calendar data to be stored on the server/cloud of the calendar provider and to be transferred to and from the calendars each time a change is made. This data transfer and storage leads to the possibility of data being intercepted on the way between cloud servers and the device with the calendar; this can be done either by companies looking to "improve their service" or by hackers or ransomware (malicious software that threatens to publicize obtained data unless a ransom is paid). Hackers, if successful, may use data retrieved from online calendars to make accurate assumptions about your whereabouts. They could break into your home or even stalk/follow you. Finally, syncing different online calendars from different sources (e.g. Google calendar and Outlook calendar) can cause automatic alterations to privacy settings. Settings can change to "public" where they might have been private on the previous calendar. When users are unaware of these setting changes, they may unknowingly be publicizing private events.

YOUR POTENTIAL ACTION **STEPS**?

FIRST STEPS:

- Revisit the privacy settings of the calendar in use
- Set strong passwords on your online calendars and change them periodically
- Avoid syncing different calendars and sharing them
- If you would like to continue syncing calendars across devices or applications, be aware of the privacy settings on each device or application and adjust them after syncing where necessary
- If you would like to share your calendar with someone be careful with whom you are sharing and the settings
- Do not set your calendar public
- Do not put your exact location for an entry in your calendar (rather, think of ways to call a certain location that are clear to you but unclear to strangers)
- Check the applications that have the authorization to access your calendar application

FOR ENTHUSIASTS:

- Consider complementing your calendar application with a layer of encryption: download and set up an application that will allow you to use your calendar application, and simply acts as an extra service within your calendar that encrypts your calendar data (for example, Fruux). Fruux is a cross-application synchronization and back-up service using encrypted SSL transfers that simply "sits" on top of the applications you already use to make them safer
- Consider an offline calendar (for example, Simple Calendar) that stores the data locally on your device and does not sync it with any account. Offline calendars do not require any data transfer or storage of data in remote servers or clouds, and so there is no risk of interception or others reading your calendar entries

Trade-offs

- Be weary: when opting for an offline calendar, there is no option to restore your data if you lose it
- There is also no option to access your calendar or contacts across several devices, so if this is a necessity, opt for another option from the list above

PRIVACY IN EMAIL APPS

RESEARCHED BY OANA & SIMIN

Google was sued in federal court in 2016 by University of California-Berkeley students and alumni, claiming that the giant who handles the university's accounts has illegally scanned and intercepted their correspondence without having any approval, in order to use it for targeted advertising. In the lawsuit it is affirmed that Google tricked not only Berkeley but other institutions too that the accounts will not be scanned in order to serve targeted advertisements; thus the users were informed by universities that their privacy is assured. Unfortunately, this is not the first time Google is the subject of this sort of accusations. A similar lawsuit was filed in 2013 for the same issue. Google not only failed to be transparent with its practices, but it illegally used student and staff data for commercial purpose.

	GMAIL	OUTLOOK	ICLOUD	RUNBOX	TUTANOTA
INFORMATIONAL CONTROL	□🟥□□□□□	□🟥□□□□□	□🟥□□□□□	□□□□□□🟩	□□□□□□🟩
DECISIONAL CONTROL	□🟥□□□□□	□□🟧□□□□	□□🟧□□□□	□□□□□□🟩	□□□□□□🟩
BEHAVIORAL CONTROL	□□🟧□□□□	□□🟧□□□□	□□🟧□□□□	□□□□□🟩□	□□□□🟩□□
PRIVACY FRIENDLY DEFAULTS	🟥□□□□□□	□🟥□□□□□	□□□🟨□□□	□□□□□□🟩	□□□□□□🟩
TECHNOLOGY PATERNALISM	□□□🟨□□□	□□□🟨□□□	□□□🟨□□□	□□□□🟩□□	□□□□□🟩□
PRIVACY BY DESIGN	□□🟧□□□□	□□🟧□□□□	□□🟧□□□□	□□□□□🟩□	□□□□□🟩□
SERVICE APPEAL	□□□□🟩□□	□□□□□🟩□	□□🟧□□□□	□□□□🟩□□	□□🟧□□□□

*Each bar, left to the right, represents a grade starting from very poor, poor, fair, neutral, good, very good, excellent.

EMAIL APPS - RISKS

Risks resulting from email applications are 3-fold.

1st: Sensitive information leakage: Some providers that including Google are still not fully encrypting your email traffic, that could potentially contain sensitive information such as credit card or physical address. This means that when sending an email containing such information, it is relatively simple for hackers or other intercepting parties to abuse the intercepted information.

2nd: The leakage of sender and receiver email addresses: Even where the body and attachment of an email may be encrypted, sender and receiver addresses are usually not. This could potentially cause you being spammed and provide the enter point for being hacked.

3rd: Your provider might mine your emails and sell the gathered data to a 3rd party for profit. You will need to look at advertisement in your email inbox window and you will have your data exposed in data trading between the email provider, advertisers and non-obvious parties.

YOUR POTENTIAL ACTION **STEPS?**

FIRST STEPS:

If you are concerned about your privacy, what happens to your data and what you can do towards being more secure while using the e-mails services, but you do not want to invest too much time and resources in this area, here are some first steps you can take:

- First and foremost, make sure your password is secure enough. It should be at least 8 to 10 characters, including letters, digits and special characters. Also, it is advised to regularly change it
- Use a secure connection. E-mail services allow you to change settings and to use an encrypted "HTTPS" connection, instead of the "HTTP" one
- Never open attachments or click on links received from suspicious senders. No matter how tempting that offer sounds, always double check everything

FOR ENTHUSIASTS:

Apart from the options mentioned above, there are further steps to take to ensure your privacy and safety if you're ready for a bigger change to protect yourself:

- Register for a paid privacy-friendly email provider that doesn't rely on your data for their business model
- Register your email in a country with better privacy regulations and manage your traffic through VPN, this avoids the government spying on you
- Use the PGP protocol instead the standard email traffic protocols, the message body and attachments are then well encrypted
- A private email server is a good option. You can set up your own server, encryption, and since you own it, there will be no Google to breach your privacy, with your own encryption you can store your data at the site of your provider safely

The most bullet-proof solution only if you are a programmer, write your email client that ensures no backdoor/trackers and in addition your private email address with VPN traffic protection. This should exempt users from most of the attacks/leakages.

Vienna University of Economics and Business
The Institute for Management Information Systems
Welthandelsplatz 2, 1020 Vienna, Austria

January, 2018

WIRTSCHAFTS
UNIVERSITÄT
WIEN VIENNA
UNIVERSITY OF
ECONOMICS
AND BUSINESS

PRIVACY &
SUSTAINABLE
COMPUTING LAB