Privacy and security of COVID-19 contact tracing in Belgian catering

Non Peer-reviewed author version

DOI: 10.13140/RG.2.2.15339.26403
Handle: http://hdl.handle.net/1942/34272

Privacy and security of COVID-19 contact tracing in Belgian catering

Mariano Di Martino

Hasselt University - tUL, Expertise Centre for Digital Media (EDM)
mariano.dimartino@uhasselt.be
Technical report

1 Introduction

On July 24th, the minister of Security and Interior in Belgium has published a Ministerieel Besluit (MB) [2] that contains several provisions on how the visitors of cafes and restaurants should behave in order to prevent the spread of COVID-19 and to trace human contacts between (potentially) contagious people. In this paper, we focus on the following article in the MB that is enforced when a cafe or restaurant receives clients (translated from Dutch):

> *Art. 3. § 10: The contact information of one customer per table, which can be limited to a phone number or email address, must be registered at arrival and must be kept for 14 days in order to facilitate future contact tracing. This contact information can only be used for the objectives against COVID-19, they must be destroyed after 14 days and the customers must give explicit permission. Customers who deny, will not be allowed to use the establishment of the cafe or restaurant.*

This article became enforceable starting July 25th until October 19th 2020, when the corresponding article became obsolete [3, Art.6 §1].

2 Methodology

We visited 10 cafes and restaurants (which we refer to as 'caterers') in Belgium and observed the method they use to request the necessary contact information and subsequently examined from which source (e.g. websites) these methods are coming from. In this manner, we analyze 2 privacy aspects. First, we analyze whether the contact information is *only* used for contact tracing and therefore should not be used for commercial activities such as advertisements. This is performed by providing each caterer with a unique honeytoken that contains an email address and phone number. We then observe each email address and phone number for a period of 120 days, to potentially capture messages that are not used for contact tracing. Note that we essentially visited and ordered drinks and/or food of each caterer, and did not disclose our research to not raise any suspicion.
Secondly, we evaluate the potential privacy and security issues of the online

platforms that are used by some caterers to handle and save the customer's contact information.

3 Results

Table 3 shows the 10 caterers that we observed. 3 out of the 10 caterers requested the information to be written on an empty piece of paper or the back of a beer mat. While 1 caterer did not request the necessary contact information at all. Furthermore, 3 caterers requested the customers to provide their contact information through an online website by scanning a QR code and only one caterer used a physical form provided by the government [1], which each customer should fill in by hand. Finally, 2 caterers provided each customer the same piece of A4 paper that contains the contact information of multiple customers, thus clearly not protecting this sensitivity of this information. In addition, we noticed that platform Y has a similar A4 paper for filling in contact information. We argue that such method is not conform to privacy by design principles.

Fortunately, for the honeytoken approach, we did not capture any message on our email addresses or phone numbers for a period of 120 days.

However, when analysing the 2 online platforms used for contact tracing, we have discovered some minor privacy issues as well as multiple significant security vulnerabilities, which are discussed below. First, we start with platform X, which has a customer base of at least 100 caterers:

- Platform X had a very minimal privacy policy listed on the website which did not mention cookies, although cookies were used when filling in the contact information through that platform. It is therefore unknown for which purpose these cookies are created.
- Platform X allowed the customer to change the check-in date by simply modifying a specific HTTP POST request parameter, bypassing the main objective of having an accurate method of contact tracing.
- A customer of platform X was able to perform a virtually unlimited number of check-ins remotely.

Next, we discuss platform Y, which has a customer base of at least 600 caterers:

- We observed a security vulnerability that allowed any customer to see the total number of registrations for each caterer, the timestamp of each registration, as well as a censored version of the email address of each customer (only the first and last letter of the local part of the email address and the domain name were visible).
- We observed that the retention period of platform Y was 28 days, instead of 14 days as listed in the MB. Later, the developer of the online platform privately mentioned that the 28 days was fixed for every caterer in any province because the retention period of a specific province in Belgium (Antwerp) had a exception to that rule, which was 28 days.

– Platform Y had a vulnerability that allowed any customer to remove the internal form of any caterer, meaning that none of the customers would be able to fill in the form without the caterer re-adding the form on the online platform.

All vulnerabilities were responsibly disclosed to the appropriate developers and were ultimately all fixed.

Table 1. Lists all the observed caterers and their corresponding method and/or online platform.

Caterer	Method	Online platform
A	Back of beer mat	
B	QR code	Platform X
C	QR code	Platform X
D	Small piece of paper	
E	Nothing	
F	A4 paper with multiple customers	Unknown
G	Small piece of paper	
H	Piece of paper issued by government	
I	A4 paper with multiple customers	Platform Y
J	QR code	Platform Y

l

References

1. Aanwezigheidsformulier COVID-19 - Gasten Horeca. *Federal Government - Economie* (July 2020). https://economie.fgov.be/sites/default/files/Files/Entreprises/formulaire-horeca-formulier-vlaanderen.pdf.
2. Ministerieel besluit houdende wijziging van het ministerieel besluit van 30 juni 2020 houdende dringende maatregelen om de verspreiding van het coronavirus COVID-19 te beperken. *Belgisch Staatsblad* (July 2020). Numac: 2020031150.
3. Ministerieel besluit houdende wijziging van het ministerieel besluit van 30 juni 2020 houdende dringende maatregelen om de verspreiding van het coronavirus COVID-19 te beperken. *Belgisch Staatsblad* (Oktober 2020). Numac: 2020031557.