doi: 10.36689/uhk/hed/2021-01-073

Is Citizen Tracking Acceptable?

Jana SYROVÁTKOVÁ*and Antonín PAVLÍČEK

Prague University of Economics and Business, Prague, Czech Republic; jana.syrovatkova@vse.cz; pavlicek@vse.cz

* Corresponding author: jana.syrovatkova@vse.cz

Abstract: Along with the extensive use of information and communication technology (ICT) gains importance also the issue of privacy. The main questions are: a) how much invasions of privacy and b) from whom is still acceptable. In this paper, we discuss the approval of invasion of privacy from state institutions (government and police). The research took place in the Czech Republic in October 2020, out of 429 respondents 302 were first-year university students. Paper answers whether people agree with invasion of privacy by state institutions. Alternatively, which interventions they consider to be tolerable and where their disagreement is significant. Due to the COVID epidemic, the question of automatic monitoring of the spread of the epidemic was included. Privacy intrusion was divided into 4 categories - police information, security, gathering information for scientific and other beneficial purposes, information about citizens interfering with privacy or without a clear purpose. The answers are further differentiated according to age and gender. The perception of individual intrusions on privacy by different groups is compared. Main findings include an agreement to share data for scientific purposes and strong disagreement with the automatic evaluation of tweets in order to monitor the spread of epidemics. Research shows that people generally disagree with automated invasions of privacy.

Keywords: e-government; tracking; survey

JEL Classification: H76; O38; H12

1. Introduction

The fundaments of modern systematic surveillance of population were laid by cardinal Richelieu in 17th century, but culminated in the era of French Revolution. At that time, they did not have the current technological possibilities for monitoring and recording, instead it was achieved through the Comité de surveillance révolutionnaire - a network of informants and prosecutors. Seemingly innocuous data about citizens has been misused many times in the past. A sad example are membership lists of Sokol and The Jewish community, which were acquired by the Gestapo in 1939 and abused for liquidation of "unsuitable" persons. The Russian counterintelligence acted similarly in 1945, equipped with lists of Russian emigrants (Vokoun, 2020).

In connection with the expansion of information and communication technologies (ICT) and the possibilities of automated monitoring of citizens almost "at every step", the topic of privacy is widely discussed. There are appeals to privacy as a right to decide with whom to share what information. Great emphasis is placed on the protection of information about one's own social ties, which have been misused many times in the past to persecute people who knew uncomfortable people (Vokoun, 2020).

One of the reasons of Bitcoin's popularity is its anonymity – it provides privacy of ownership, as well as of transactions - the payments are not traceable (Sudzina et al., 2019).

On the other hand, there is a very common approach: "He who does nothing wrong, has nothing to hide." Some security oriented apps can actually help user to record the details of his life in the protected Timeline, which contains information such as who, when, and where the user is meeting, just in case anything happens. User can add his friends to so called Safety Network so they can make sure user never goes missing (Noonlight, 2021). The app can be pre-programmed for how long user would like to be tracked. It can also store the details about his time – pictures, notes. If the user does not confirm his/her safety in regular intervals, it would automatically send an alert to the friends with exact location (Watchovermeapp, 2021). It can also make live stream, share the current location, and guardians can trace the user via GPS (BSafe, 2021).

At the Philippines users can install Android application AppLERT which can help victims of the natural or man-made disaster to seek help. Users can also notify others of the danger ahead through application or through Facebook. Application uses built-in GPS in the user's mobile phone (Fabito et al., 2016).

Terrorists and criminals are big phenomena in human society. Governments try to organize activities such as TAKEDOWN Project (EU H2020), which is focused on the understanding of Organized crimes and Terrorism phenomena with the aim to deliver cyber solutions by focusing on an advanced collaboration among citizens and Law Enforcement Agencies (Tundis et al., 2020).

It is very difficult to decide where the limit lies, what is acceptable and permitted surveillance and what is already an unwanted invasion of privacy. What some think is right, others will consider inadmissible. In the context of the COVID-19 epidemic, the European Data Protection Board approved a Request for mandate regarding geolocation and other tracing tools in the context of the COVID-19 outbreak, which directly explains what is and is not permissible epidemic surveillance (EDPB, 2020).

2. Methodology

We have collected data in November 2020 as a part of the larger survey focused on social networks and privacy. Respondents were the first-year students of Prague University of Economics and Business, Faculty of Finance and Accounting (N = 299) and various students of the Faculty of Informatics and Statistics (N = 130).

We had analyzed the perception of individual intrusions on privacy by different groups. The answers are further differentiated according to age and gender. For statistical analysis we had used t-test with H0: $\mu_0 = 5.5$ resp. $\mu_0 = 50$ depending on question type and with HA: $\mu_0 \neq 5.5$ resp. $\mu_0 \neq 50$. We had set confidence intervals for μ too.

For comparisons between types of respondents we had used t-test too. In that case was H0: $\mu_1 = \mu_2$ and HA: $\mu_1 \neq \mu_2$. We set also confidence intervals.

Results are sumarized in the form of descriptive pie charts, bar charts and cobweb charts.

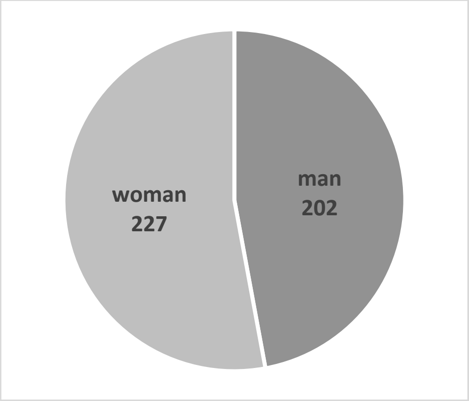

Figure 1. Gender of respondents

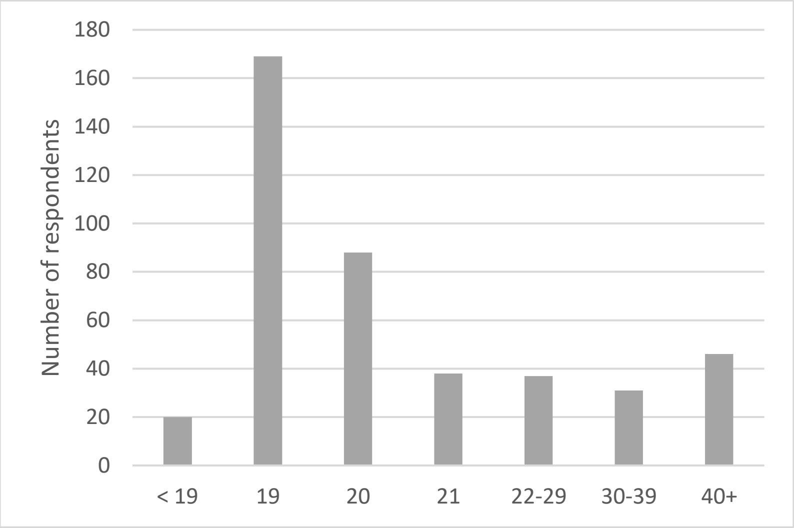

Figure 2. Age distribution of respondents.

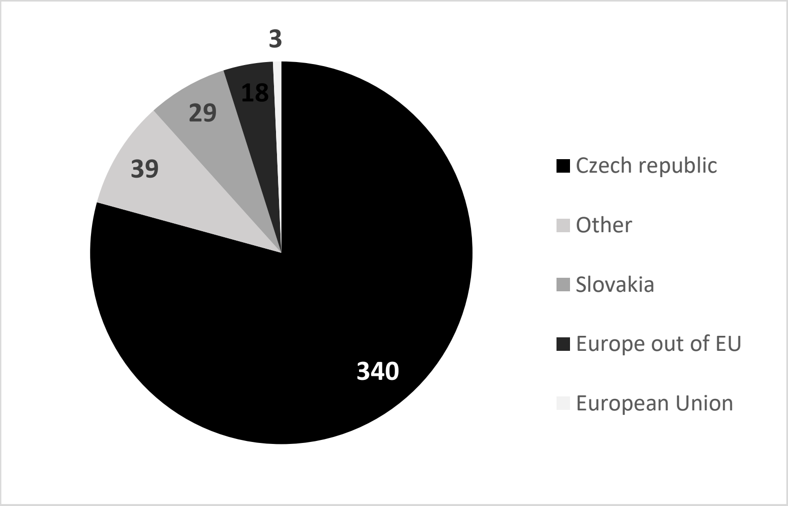

Figure 3. Birthplace of respondents.

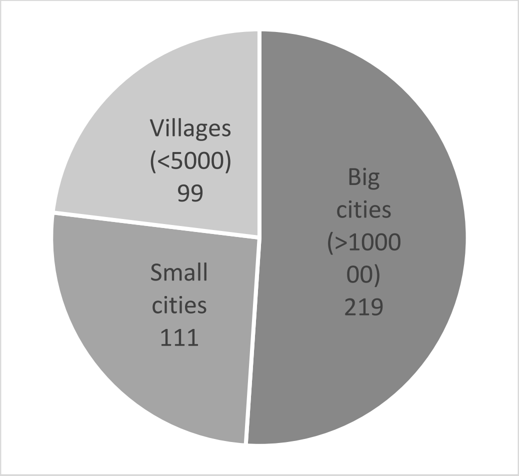

Figure 4. Urbanization of respondents

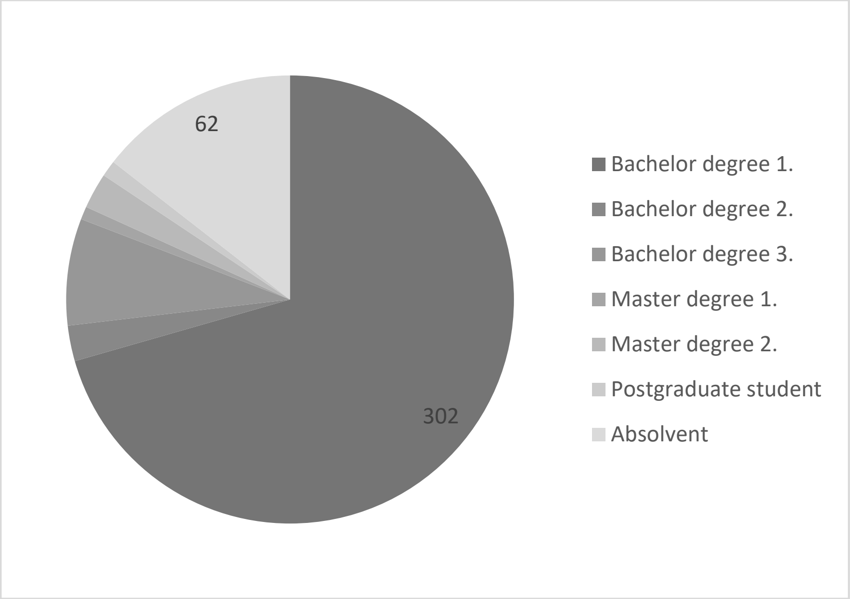

Figure 5. School year distribution of respondents

Article analyzes 10 questions related to 4 categories: a) scientific and other seemingly beneficial purposes, b) information about citizens interfering with privacy with or c) without a clear purpose, d) security, police information. We code questions Q1 to Q10. Respondents were asked how much they agree or disagree with the statement on likert scale of 1 to 10 from strongly agree to (1) to strongly disagree with the sentence (10).

2.1. Survey Questions

Science and altruism

- Q1 Movements of drivers' mobile phones (geolocation) should be monitored by the Ministry of Transportation to analyze the usage of transport infrastructure and to predict traffic congestion.
- Q2 All state-owned / managed data should be freely available for scientific and research purposes.

- Q3 Data from mobile applications, search engines and social networks should be used to solve serious social problems (security, unemployment, immigration, etc.).

Informing citizens

- Q4 The government should be able to monitor and analyze mobile phone location data to find out where individuals actually live and work.
- Q5 Automated detection of unusual (dangerous) behavior at airports / train/bus stations / in public transport may include profiling according to age, gender and ethnic origin or expressions of faith.

Safety

- Q6 Tweets or searches with words such as "vomiting", "temperature", "headache" should be used to monitor the spread of the viral disease epidemic.
- Q7 Encrypted communications (i.e. Telegram app) should be banned to make it easier for the government to detect security threats.

Police

- Q8 Drivers for whom the monitoring of the movement of their telephone detects a significant speeding or other dangerous behavior (violation of the entry ban, ...) should be automatically penalized. (data passed to the police)
- Q9 The police should have easy access to a list of telephone calls.
- Q10 The police should be able to monitor the movement of people through their mobile phone.

3. Results

The following graph shows a summary of all answers. It can be seen that people usually disagree with monitoring. For some questions it is less pronounced, for example Q1, while for Q4 the disagreement is really strong.

The basic statistical analysis of the whole dataset is in Table 1. In addition to t-statistics, the confidence interval for the mean is added to illustrate possible fluctuations of the mean value estimates of individual questions.

It is therefore clear from the results that hypothesis H0 for this question cannot be rejected for Q1. The answers are not significantly skewed to either side. Therefore, the data show that aside from the use of mobile phones for location tracking to prevent traffic, people are divided. All other equality hypotheses can be rejected because the test statistic is higher than 1.96. The most significant deviation is in question Q4 followed by question Q7 aimed at prohibiting encrypted communication. Other significant disagreements are issues related to police surveillance of mobile phones and twitter communication in order to combat epidemics.

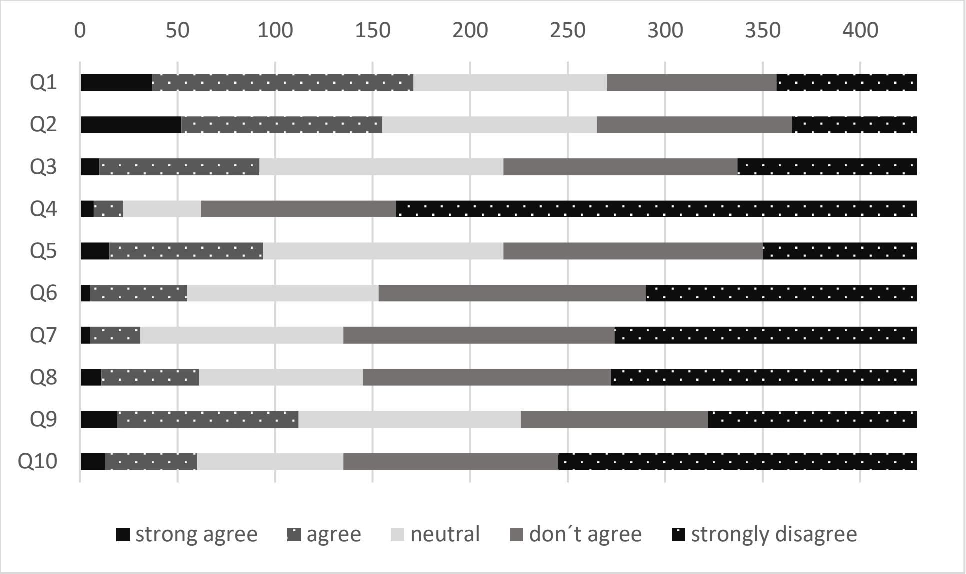

Figure 6. Summary chart of agreement and disagreement with the statements

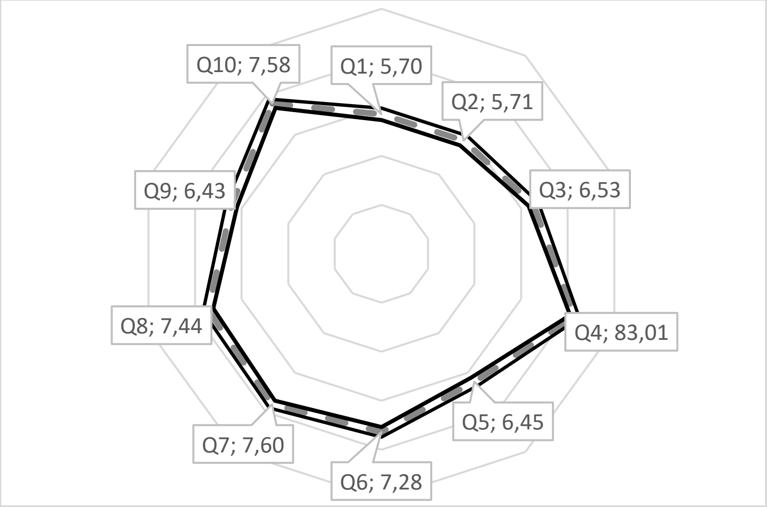

Figure 7. Confidence interval and mean for whole dataset

Table 1. Statistical analysis of the whole dataset

		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean		5.70	5.71	6.53	83.01	6.45	7.28	7.60	7.44	6.43	7.58
sampling variance		6.38	6.54	5.11	446.29	4.88	4.72	4.04	5.41	6.09	5.55
t-statistics		1.63	1.71	**9.43**	**32.36**	**8.95**	**16.94**	**21.59**	**17.25**	**7.82**	**18.31**
confidence interval for the mean	**min**	5.46	5.47	6.32	81.01	6.25	7.07	7.41	7.22	6.20	7.36
	max	5.94	5.95	6.74	85.01	6.66	7.48	7.79	7.66	6.66	7.81

3.1. Analysis for Different Groups of Respondents

In the next part, we analyzed the data by gender and age. As the basic research took place among first-year students, they are all under the age of 20, while others are 21 and older. Also, in this analysis, we have focused on the mean value and hypotheses whether the mean value is significantly skewed to either side.

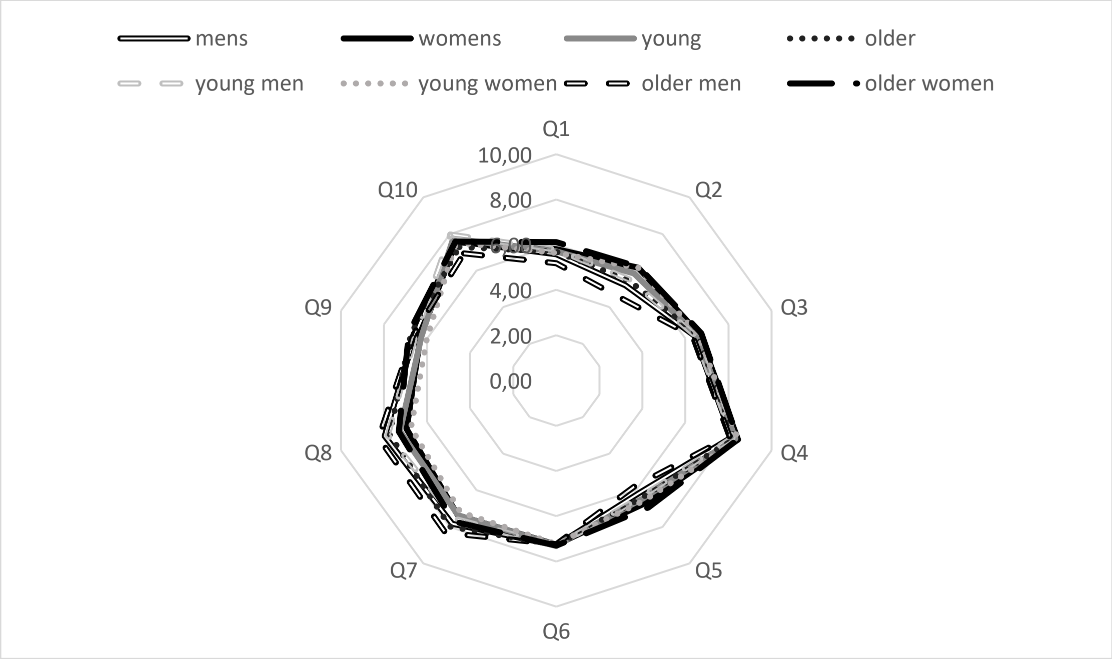

Figure 8. Differences of the mean depending of the sex and age

Table 2a. Differences of the mean depending of the sex and age

	Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	Q10
Men	5.58	5.20	6.41	81.4	6.18	7.30	7.84	7.98	6.57	7.61
Women	5.81	6.17	6.63	84.4	6.70	7.26	7.38	6.96	6.31	7.56
Young	5.70	5.85	6.52	83.2	6.47	7.28	7.38	7.26	6.26	7.74
Older	5.69	5.46	6.55	82.6	6.42	7.28	7.99	7.75	6.74	7.29
young men	5.79	5.52	6.45	81.9	6.37	7.33	7.58	7.83	6.54	7.97
young women	5.63	6.15	6.58	84.4	6.57	7.23	7.20	6.75	6.01	7.54
older men	5.19	4.60	6.34	80.5	5.81	7.24	8.33	8.26	6.63	6.94
older women	6.12	6.20	6.73	84.4	6.94	7.30	7.71	7.32	6.84	7.59

Table 3b. Differences of the means depending of the sex and age

	Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**
Men	*0.44*	*-1.68*	5.57	19.40	4.38	11.65	16.41	17.39	6.04	12.30
Women	*1.86*	4.05	7.76	26.98	8.24	12.27	14.33	8.88	5.03	13.57
Young	*1.33*	2.38	7.52	26.80	7.17	13.58	15.53	12.46	5.07	16.36
Older	*0.95*	*-0.18*	5.67	18.23	5.35	10.08	15.75	12.38	6.41	8.95
young men	*1.29*	*0.07*	4.64	16.52	4.27	9.47	11.70	13.17	4.77	12.64
young women	*0.60*	3.37	6.00	21.69	5.87	9.71	10.33	5.99	2.47	10.64
older men	*-1.02*	**-2.97**	3.06	10.35	*1.41*	6.74	12.35	11.55	3.68	4.52
older women	2.42	2.30	4.90	15.95	5.92	7.45	10.27	6.98	5.42	8.39

Table 2b proves, that hypothesis of a neutral relationship to the relevant statement for a given group of respondents cannot be rejected. In one case, we even reject the hypothesis because the data are skewed to the opposite side, i.e. it can be said that older men agree with the availability of data for scientific purposes.

There are significant differences in the results of question 2, so we have also charted the differences in confidence intervals for individual groups in the form of a ray graph in Figure 9. To highlight the differences, the scale is only from 3 to 7.

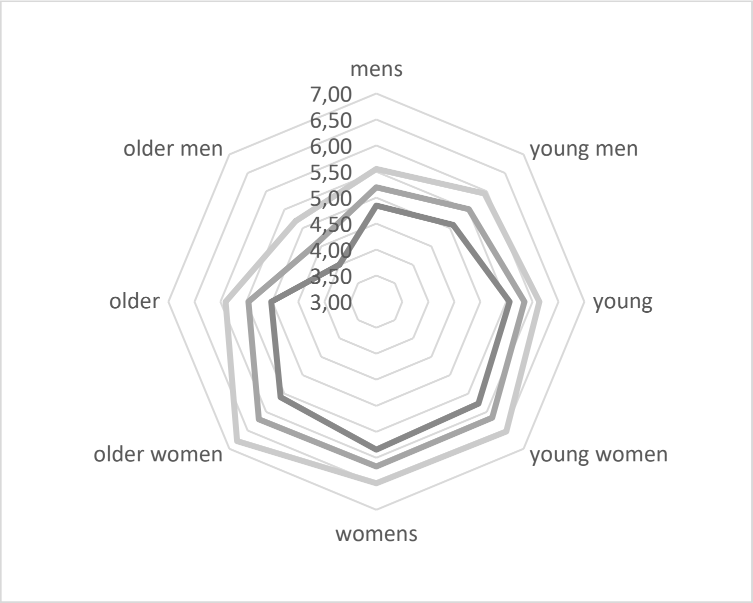

Figure 9. Differences in confidence intervals for individual groups in Q2

3.2. Differences between Men and Women, Between Younger and Older Respondents

Finally, we hypothesized whether men respond as well as women and whether young respond in the same way as older.

Table 4. T-test values for hypothesis about the same means at different types of respondents

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
men vs. women	0.93	3.99	1.02	1.47	2.46	-0.18	-2.34	-4.64	-1.09	-0.26
young vs. older	-0.05	-1.50	0.16	-0.30	-0.23	-0.01	3.06	2.08	1.95	-1.92

If we compare T-values with a critical value of the t-distribution (1.96), we can see that the differences between younger and older respondents are usually insignificant. The only difference is between questions Q7 and Q8 concerning the banning of encrypted communication and speeding monitoring by mobile phones. Both groups disagree, but the disagreement among the elders is more pronounced. Men and women also differ on these issues, with men disagreeing more.

However, men and women differ in question 2, which was discussed in more detail in the previous section, as well as in question 5 on the automatic detection of suspicious behavior at airports, and whether this detection may include race, age or gender.

4. Discussion

The paper dealt with a survey of the approach of respondents, primarily students, to monitoring/surveillance of citizens by various state institutions. The questions focused on surveillance for scientific purposes, surveillance of citizens for general undefined reasons or for security reasons, either for protection against epidemics or surveillance of mobile phones for automatic transportation fines and for more serious criminal offenses.

The survey showed that depending on the type of question, the acceptance of the observation varies, but the answers have always been skewed towards disagreement with the statement – meaning disagreement with the surveillance. Only for questions where the whole society would directly benefit from the data (scientific purposes or prediction of traffic congestion) is this disagreement not statistically significant.

Most people do not agree with non-anonymized mobile phone tracking - both in order to find out where they actually live (the most significant disagreement) and in order to be able to fine for inappropriate behavior.

When comparing data between different groups of respondents, there is an interesting discrepancy between the availability of data for scientific purposes and a discrepancy with the distinction between age, gender, ethnic origin or religion in the automated detection of dangerous behavior. Interestingly, objection to the surveillance for this reason was more profound with women. There was also disagreement with the ban on encrypted communication and automatic fines for speeding by mobile phone. The men here predictably disagreed more.

Interestingly, young and older differed little on most issues, while men were much more pronounced than women, often in all age groups.

5. Conclusions

People in general reject surveillance and monitoring. There were some exceptions (cases where the whole society would directly benefit from the data) and we have also recorded gender differences, but in general, research has proven that people largely disagree with automated invasions of their privacy.

Acknowledgments: Paper was processed with support of grant IGA no F4/13/2021 at the Faculty of Informatics and Statistics of the Prague University of Economics and Business.

References

Bsafe. (2021). Retrieved January 9, 2021 from https://getbsafe.com/

EU H2020 TAKEDOWN Research Project. (2019). https://www.takedownproject.eu/

Fabito, B. S., Balahadia, F. F., & Cabatlao, J. D. N. (2016). AppLERT: A mobile application for incident and disaster notification for Metro Manila. *2016 IEEE Region 10 Symposium (TENSYMP)*, 288–292. https://doi.org/10.1109/TENCONSpring.2016.7519420

Noonlight. (2021). Retrieved January 9, 2021 from https://www.noonlight.com/

Sudzina, F., & Pavlicek, A. (2019). Impact of Personality Traits (BFI-2-XS) on Use of Cryptocurrencies. In P. Maresova, P. Jedlicka, & I. Soukal (Eds.), *Hradec Economic Days 2019* (pp. 363–369). https://doi.org/10.36689/uhk/hed/2019-02-037

Tundis, A., Kaleem, H., & Mühlhäuser, M. (2020). Detecting and Tracking Criminals in the Real World through an IoT-Based System. *Sensors*, *20*(13), 3795. https://doi.org/10.3390/s20133795

Vokoun, R. (2020). Diktatura versus totalita, surveillance - a kde je svoboda? KSP20: Totalita včera, dnes a zítra. https://www.youtube.com/watch?v=1EsHBxim4KQ

Watch over Me. (2020). Retrieved January 9, 2021 from http://watchovermeapp.com/