EDGELANDS institute

Citizen Science for Tri-Sector Response

Participatory Citizen Sentiment Crowdsourcing Study in Geneva

Quels sont les dangers qui menacent votre sécurité à Genève ?/
What are the dangers that threaten your safety in Geneva?

In partnership with

Soul Probe

EDGELANDS institute

Contents

Résumé

Comment comprendre la perception de la sécurité des habitants de Genève ? L'Institut Edgelands a cherché à répondre à cette question dans son deuxième emplacement pop-up à Genève. Dans l'esprit de la recherche participative basée sur la communauté (CBPR), l'équipe a mené une série d'entretiens, de groupes de discussion et de débats avec des universitaires, des étudiants, des partenaires médiatiques, des experts en recherche et des citoyens pendant environ 1 mois afin de formuler 15 énoncés de base et 7 QCM pour une enquête participative et émergente qui a été lancée le 20 juin 2022. Après avoir examiné la série initiale de résultats obtenus auprès de 182 participants, l'équipe de recherche a validé 2 déclarations et 1 QCM supplémentaires le 18 juin 2022. supplémentaires et un QCM supplémentaire le 18 juillet 2022. La conversation s'est terminée le 15 novembre 2022 avec 414 répondants.

L'étude a révélé 3 groupes d'opinions ou « tribus » différents. Le groupe A (22 % des 414 répondants) se sentait en sécurité par rapport à la majorité des répondants du groupe B (53 % des répondants) qui se sentent craintifs et peu sûrs. Le groupe C (22 % des répondants) étaient soit indécis, soit craintifs quant à la sécurité à Genève. L'enquête a révélé un manque de confiance modéré dans les institutions publiques et une grave méfiance à l'égard des grandes entreprises technologiques.

Afin de quantifier et de comparer les perceptions de la peur, nous avons classé les craintes relatives à 7 questions dans un « axe de la peur »., Il en ressort que la crainte de l'utilisation des données personnelles par les grandes entreprises technologiques est la plus élevée, suivi par les algorithmes, puis la surveillance, les fraudes numériques, l'utilisation abusive des données personnelles par le gouvernement ; et enfin la peur de la sécurité physique.

Nous avons créé un autre « axe d'accord » ou « axe d'approbation publique » qui montre que la confiance dans la compétence des autorités à protéger la vie numérique était la plus faible, suivie de la confiance dans la fiabilité et l'efficacité des médias sociaux, puis le sentiment de sécurité face à des autorités qui utilisent davantage de technologies pour protéger les citoyens. La dépendance et

la capacité d'attention contribuant à un problème de santé publique ont recueilli le plus grand nombre d'avis favorables, suivies de la perception que les personnes à Genève ne signalent pas les délits numériques ; la possibilité d'envisager une « panne » de service numérique ; le sentiment d'être submergé par la numérisation de la vie urbaine et sociale ; la difficulté de remplir des formulaires gouvernementaux numériques ; et enfin, le fait d'accepter que les données personnelles collectées par le gouvernement soient stockées à l'étranger.

Cinq questions ont suscité de fortes divisions et ont justifié un plus grand débat public et la recherche d'un consensus dans la société. Il s'agit des questions suivantes : la numérisation accrue de la vie urbaine et sociale, la crainte d'être victime de fraudes numériques ; la crainte d'une utilisation abusive des données personnelles par le gouvernement genevois ; la crainte de l'utilisation de plus de technologie par la police et le gouvernement ; et enfin, l'efficacité du partage des incidents sur les médias sociaux par rapport au signalement aux autorités.

Dans l'ensemble, l'âge et le statut de séjour sont deux marqueurs identitaires ou démographiques importants qui expliquent certaines différences dans la façon dont les répondants ont voté. Les commentaires qualitatifs ont révélé des couches complexes de nuances et de textures qui laissent entrevoir les causes profondes des problèmes à résoudre, par exemple le fossé socio-économique, le fossé des classes ou le fossé croissant de la culture numérique.

En nous inspirant de l'« axe de la peur », de l'« axe de l'accord », de la matrice de décision et des commentaires du public, nous avons dressé une liste de 19 recommandations détaillées sous 9 grands thèmes de recommandations de haut niveau. Nous avons visualisé ces recommandations dans une matrice 3X3 qui représente 3 acteurs différents de la société qui pourraient agir sur plusieurs points d'action selon trois niveaux de priorité. Nous concluons ce résumé par six des recommandations les plus importantes.

Premièrement, il y a un sentiment de résignation ou d'« impuissance acquise » face à un pouvoir qui penche trop favorablement dans les mains des grandes entreprises technologiques. La société a besoin d'une force compensatrice pour tenir en échec les intérêts des grandes entreprises technologiques. Un

partenariat trisectoriel « public-peuple-privé » de processus de démocratie délibérative (par exemple à Taiwan) ou de comités d'examen et de panels de citoyens qui explorent et sensibilisent le public aux nuances des arguments de toutes les parties prenantes pourrait aider la société à progresser plus délicatement et plus habilement vers un consensus sur ces questions. Des audits indépendants de la transparence et de l'utilisation correcte des données personnelles par les grandes entreprises technologiques contribueraient à apaiser les craintes des citoyens.

Deuxièmement, les autorités doivent faire davantage pour regagner la confiance de la population. Les autorités doivent se développer et démontrer leur compétence à protéger la vie numérique des citoyens. Elles doivent veiller à la bonne utilisation des données personnelles des citoyens et des résidents et apaiser les craintes des citoyens quant à la présence accrue de la surveillance numérique dans leur vie quotidienne.

Troisièmement, les réponses de la justice et des services répressifs n'ont pas été suffisamment développées pour faire face aux crimes numériques qui évoluent à un rythme beaucoup plus rapide. Il est urgent que les citoyens et les résidents soient informés de leurs droits sur leurs données et des voies de recours en cas de violation de ces droits. Une meilleure coordination entre la police, le système judiciaire et les citoyens est nécessaire pour répondre rapidement à la nature évolutive des menaces numériques.

Quatrièmement, la dépendance aux technologies, la réduction de la durée d'attention, la peur des algorithmes et leur impact sur la santé publique constituent une « bombe à retardement » prête à exploser dans un avenir proche si nous ne prenons pas de mesures préventives ou proactives pour résoudre le problème. Les commentaires semblent suggérer que le problème est hors de contrôle et très complexe, ce qui nécessite la coopération de multiples parties prenantes.

Cinquièmement, la société devrait se réunir pour discuter de la manière dont la fiabilité des médias sociaux en tant que source d'information et de sensibilisation aux menaces pour la sécurité à Genève pourrait être améliorée, ainsi que de la

manière dont ils pourraient compléter les canaux de signalement formels auprès des autorités. autorités. Il s'agit d'un domaine de développement naissant qui nécessite une délibération plus concertée entre la population, le secteur public et le secteur privé, qui pourrait être mise à l'épreuve par une série d'exercices de planification de scénarios.

Sixièmement, il existe dans la population une proportion importante de personnes âgées et de minorités non alphabétisées dans le domaine du numérique qui ont du mal à remplir les formulaires administratifs numériques. Il convient d'adopter un cadre d'élaboration des politiques fondé sur la philosophie du « centrage des marges » afin de combler le fossé entre les personnes ayant une culture numérique et celles qui n'en ont pas. Il s'agirait par exemple d'offrir une assistance humaine plus importante pour ces services et de concevoir des formulaires numériques centrés sur l'humain dont la conception UI/UX est optimisée pour ces minorités.

Executive Summary

How do we understand the perception of security of the residents in Geneva? Edgelands Institute sought to answer this question in its second pop-up location in Geneva. In the spirit of community-based participatory research (CBPR)[1], the team conducted a series of interviews, focus groups and discussions with academia, students, media partners, research experts and citizens for about 1 month to distil 15 seed statements and 7 MCQs for a participatory and emergent survey that was launched on 20th June 2022. After reviewing the initial set of results from 182 participants, the research team enabled 2 additional seed statements and 1 additional MCQ on 18th July 2022. The conversation ended on 15th November 2022 with 414 respondents.

The study revealed 3 different clusters of opinions or tribes. Group A (22% of 414 respondents) felt safe and secure in comparison to the majority of the respondents in Group B (53% of respondents) who felt afraid and insecure. Group C (22% of respondents) were either undecided or afraid about security in Geneva. The survey revealed a moderate lack of trust in public institutions and a serious mistrust of big tech companies.

To quantify and compare perceptions of fear, we ranked the fears of 7 issues in an 'Axis of Fear'. It revealed the fear of use of personal data by big tech was the highest; followed by algorithms; then surveillance; digital frauds; improper use of personal data by the government; and lastly the fear of physical security.

We created another 'Axis of Agreement' or 'Axis of Public Approval' which showed that the trust in the competence of authorities to protect digital life was the lowest; followed by trust in the reliability of and effectiveness of social media and then feelings of security with authorities using more technology to protect citizens. Addiction and attention span contributing to a problem for public health registered the highest agreement; followed by the perception of people in Geneva not reporting digital crimes; the possibility of envisaging a digital service 'outage'; the feeling of overwhelm from the digitalisation of urban and social life; the

[1] Minkler, M., & Wallerstein, N. (Eds.). (2011). Community-based participatory research for health: From process to outcomes. John Wiley & Sons.

difficulty of filling digital government forms; and finally, agreeing that personal data collected by government be stored overseas.

There were 5 issues that were highly divisive which warranted greater public discourse and consensus building in society. They were the following: whether the increased digitalization of urban and social life felt overwhelming; the fear of being a victim of digital frauds; the fear of improper use of personal data by the Geneva government; the fear of use of more technology by the police and government; and finally, the effectiveness of sharing of incidents on social media as compared to reporting to the authorities.

Overall, age and residency status were 2 important identity or demographic markers that accounted for some differences in the way the respondents voted. The qualitative insights from the comments revealed complex layers of nuance and texture that hinted at deeper root causes of issues that needed to be addressed e.g. socio-economic or class divide or a growing digital-literacy divide.

Using the 'Axis of Fear', 'Axis of Agreement', Decision Matrix and crowdsourced comments as inspiration, we put together a list of 19 detailed recommendations under 9 high-level broad recommendations themes. We visualised these recommendations in a 3X3 matrix which represented 3 different actors in society who could work on several action items along 3 levels of priority. We conclude this Executive Summary with six of the more notable recommendations.

First, there was a sense of resignation or 'learned helplessness' that power has tilted too favourably in the hands of big tech companies. Society needs to have a countervailing force to keep big tech interests in check. A trisector[2] "public-people-private" sector partnership of deliberative democracy processes (e.g. vTaiwan) or citizen review committees and citizen panels that explore and sensitise the public to the nuances of the arguments for all stakeholders could help society progress more delicately and artfully towards consensus on such matters. 3rd party audits of the transparency and proper use of personal data by big tech companies would help allay fears by citizens.

[2] https://hbr.org/2013/02/why-the-world-needs-tri-sector

Second, more needs to be done by the authorities to earn back the trust of the people. The authorities need to grow and demonstrate their competence to protect the digital lives of citizens. They need to ensure the proper use of personal data of citizens and residents as well as allay fears by citizens on the increased presence of digital surveillance in their daily lives.

Third, downstream justice and law enforcement responses have not developed sufficiently to cope with digital crimes that are evolving at a much faster pace. There is an urgent need for citizens and residents to be educated on their rights to their data and the pathways for recourse when their rights are violated. Better coordination between the police, judiciary and citizens is required to respond quickly to the evolving nature of digital threats.

Fourth, addiction to technologies, the reduction of attention spans, fears of algorithms, and their impact on public health are a 'ticking time bomb' ready to implode in the near future if we do not take pre-emptive or proactive steps to addressing the issue. The comments seem to suggest that the problem is out of control and very complex, thus requiring multiple stakeholders to come together to co-operate.

Fifth, society should come together to discuss how the reliability of social media as a source of information and awareness of security threats in Geneva could be improved as well as how it could complement formal reporting channels to the authorities. This is an area of nascent development that requires a more concerted people-public-private sector deliberation that could be stress-tested with a series of scenario-planning exercises.

Sixth, there is a significant proportion of elderly and digitally non-literate minorities in the population that find digital government forms difficult to fill. A policy development framework based on the philosophy of 'centering the margins' ought to be adopted to bridge the gap between those with digital literacy and those without digital literacy. One example of this would be having more human assistance for these services and human-centred design digital forms whose UI/UX design are optimised for these minorities.

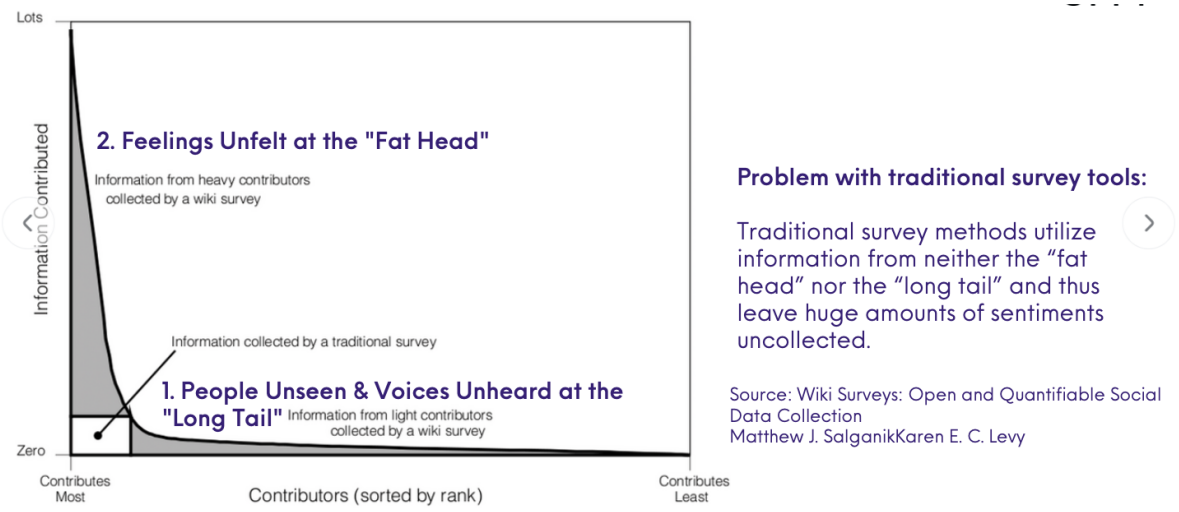
Methodology

Social Seismography

Social Seismography is a new emerging discipline of social science research, pioneered by Soul Probe (www.soulprobe.com), that uses innovative social listening tools to help leaders and citizens to gain a deeper understanding of fault-lines and glue-lines of social issues in our society. By gaining a deeper understanding of the underlying root causes, fault-lines or undercurrents that have been festering invisibly for a long time, we are able to design more effective policy, cultural and civic solutions to address these issues sustainably over the long-term before it is too late.

Within the discipline of social seismography lies the use of emergent surveys or wiki-surveys. Wiki or emergent surveys are different from traditional surveys in that they co-create the survey questions together with participants. For the purposes of this study, Soul Probe has used an AI-powered conversation platform, OPPi (www.oppi.live). Respondents to an OPPi conversation have a say in shaping the trajectory of the discourse, diagnosis or survey because survey design is both top-down and bottom-up. As illustrated in the diagram below (Figure 1), OPPi captures additional sentiments at the “fat head” and at the “long tail” that traditional survey tools are unable to capture.

Figure 1: Advantages of wiki surveys



By combining the scale and reach of a survey with the open-ended discovery of a focus group discussion, insights often surprise organisers as they challenge their preconceived ideas or cognitive biases about a particular issue. Through this unique discipline of social seismography and emergent surveys, Soul Probe helps a complex system to become more self-aware.

How does AI enable structured citizen-crowdsourcing at scale?

OPPi is an AI-powered engagement tool that leverages the power of emergent or wiki-surveys to help leaders in gathering the pulse of the people and facilitating high quality decision-making for complex societal issues. Soul Probe has been using wiki-survey tools like OPPi to bring the voices of the people and marginalised communities to decision-making tables in the public sector, parliament and private sector globally.

OPPi combines quantitative and qualitative methods with advanced statistical techniques to identify opinion tribes based on respondents' views and visualise correlations between opinions and respondents. OPPi learns patterns from respondents in real-time to help leaders identify fault lines and common ground.

How does an OPPi conversation work? What is CBPR?

Participants are given a psychological safe virtual space to answer a series of "seed statements" posed by the OPPi web platform. These "seed statements" were determined through a series of online and offline interviews, focus groups, conferences and discussions with academia, students, media partners, research experts and citizens from February 2022 to June 2022. The design of the "seed statements" was developed in line with the philosophy of community-based participatory research (CBPR).[3] We used Barbara Minto Pyramid to structure the design to cover as much breadth and depth as possible.

[3] Minkler, M., & Wallerstein, N. (Eds.). (2011). Community-based participatory research for health: From process to outcomes. John Wiley & Sons.

The survey was launched on 20th June 2022 with 15 seed statements and 7 MCQs ended on 15th November 2022 with 17 seed statements and 8 MCQs. The votes or responses of the participants are kept confidential. No one is able to trace back any individual response to any of the participants.

A moderator selectively enables comments submitted by participants as "crowdsourced statements" which circle back into the conversation for other participants to vote on. At the end of the conversation, participants are shown a real-time summary of the results of the entire conversation and which opinion group participants fall under. This has 3 benefits. First, it helps individuals in an organisation or society to cultivate self-awareness and collective awareness. Second, it shifts the ownership or burden of the issue from the organisers to the community i.e. leaders and community respondents. Third, participants start to contribute more meaningful comments and statements to build common ground with their fellow peers. OPPi has proven to "gamify" consensus building and common ground for complex conversations.

This is in sharp contrast to traditional platforms for discourse which amplify echo-chambers, silos and divisions. Often, the loudest and most provocative voices win. OPPi, on the contrary, preserves minority opinions while bringing to light the views of the silent majority. In doing so, OPPi actually levels the playing field for the loud minority and the silent majority. Overall, reviewed the comments from participants regularly, and added an additional seed statement on suicide prevention mid-way through the poll, in response to new insight generated by participants. Most other comments provided and crowdsourced among participants were aligned with existing topics and questions covered by the poll.

For the purposes of this study, the research team enabled 2 additional seed statements and 1 additional MCQ on 18th July 2022 after reviewing the survey results from 182 participants.

Survey/Poll Design

The survey was conducted in English and French in one poll environment. At the end of the survey, we asked an open-ended question to gather new perspectives from the participants: "Voulez-vous proposer d'autres questions sur ce thème? Please share additional ideas on this topic."

To keep in touch with the participants at the end of the survey we got the consent of participants to share their e-mail addresses with the following message: "Des informations sur Edgelands à Genève? Donnez votre address e-mail. Stay in touch with us by sharing your e-mail. "

Poll Timeline and Poll Participant Count:

We had set an objective of attaining 385 participants for our poll.

Phase	Date	Poll Participant Count
Poll Preparation	7th February to 7th June 2022	-
Poll Design	8th June to 19th June 2022	-
Poll Test	5pm SGT on 20th June 2022	-
Poll Launch	22nd June 2022	0
Poll Participant Count Check 1	30th June 2022	119 participants
Present 1st Interim findings to Edgelands Research team	3pm SGT on 11th July 2022	Not available
Enable 2 new seed statements and 2 new MCQ	18th July 2022	182 participants
Poll Participant Count Check 2	25th July 2022	194 participants
Reignite interest in the poll after summer holidays in Geneva	Mid August	Not available

Poll Participant Count Check 3	22nd August 2022	220 participants
Poll Participant Count Check 4	20th October 2022	289 participants
Poll Participant Count Check 5 And Final Campaign Boost	26th October 2022	302 participants
Poll End	15th November 2022	414 participants

Poll Question

Quels sont les dangers qui menacent votre sécurité à Genève ? / What are the dangers that threaten your safety in Geneva?

Poll Description:

L'utilisation croissante des technologies de surveillance vous inquiète-t-elle ou au contraire vous rassure-t-elle ?

Quelles sont vos inquiétudes sur votre sécurité à Genève à l'heure où les technologies numériques sont toujours plus présentes. Menaces physiques ? Cambriolage ? Caméra de surveillance ? Exploitations de vos données par les autorités ou les privés ? Piratage de vos ordinateurs ?

Nous vous proposons de répondre à ce sondage et de revenir ces prochaines semaines pour consulter les résultats et répondre à de nouvelles questions.

The increasing use of surveillance technologies worry you or on the contrary reassure you?

What are your concerns regarding your safety in Geneva at a time of increasing digitalization. Physical threats? Burglary? Surveillance cameras? Exploitation of your data by public or private actors? Hacking?

We invite you to take this survey, and come back in the coming weeks to answer new questions.

(Image credits: StockSnap, Pixabay)

Poll Image:

Poll MCQs / Variables:

MCQs or Survey Variables helped us to understand the demographic profile of our respondents as well as to "slice and dice" the results for the seed statements by any of the following listed variables. Participants of the poll cannot pass a demographic question unlike seed statements. The survey was launched with 7 MCQs. The 8th MCQ was added after reviewing the results from the first set of 182 participants on 18th July 2022, approximately 1 month after the official launch.

1. Age	How old are you? / Quel est votre âge ? 1) ≤ 14 2) 15 - 24 2) 25 - 34 3) 35 - 44 4) 45 - 54 5) 55 - 64 6) 65 - 74 7) ≥ 75

2. Gender	What's your gender? / Quel est votre sexe ? 1) Male 2) Female 3) Non-binary / non-conforming 4) Transgender 5) Other 6) Prefer not to respond
3. Occupation/Role	What's your sector? / Quel est votre secteur ? 1) Privacy Advocate 2) Cybersecurity 3) Security 4) Technology 5) Academia 6) NGO 7) Police 8) Journalism 9) Public Sector 10) Other
4. Citizenship/Migrationn Status	Which of the following best describes your residency status in Geneva? / Lequel des choix suivants vous décrit le mieux ? 1) Swiss citizen 2) Permit C 3) Permit B 4) Permit L 5) Other permit 6) No Permit
5. Responsibility	Which of the following should be mainly responsible for your digital security? / Laquelle des entités suivantes devrait avoir la principale responsabilité de ma sécurité numérique ? 1) Myself 2) The Geneva authorities 3) The federal government 3) Private companies 4) The European Union 5) Others

6. Perception of data being collected *Note: This was the only MCQ that allowed participants to choose more than 1 option	What kinds of data do you think is being collected about you? You may select more than 1 option. / Selon vous, quels types de données sont collectés sur vous et à votre sujet ? Vous pouvez sélectionner plus d'une option. 1) Les images des cameras de surveillance / Video footage 2) Ma localisation / Data about my location 3) La reconnaissance faciale / Facial recognition 4) Mes historiques d'achat / Purchase history 5) Les historique de ma navigation sur internet / Browsing data 6) Others
7. Location	Vous habitez où en ce moment? / Where do you currently live? 1) Geneva 2) French speaking region of Switzerland apart from Geneva 3) German speaking region of Switzerland 4) Italian speaking region of Switzerland 5) Romansh speaking region of Switzerland 6) Outside of Switzerland but still within Europe 7) Outside of Europe
8. Trusted Actors *Note: This MCQ was added	Parmi les acteurs suivants, auxquels faites-vous le plus confiance pour gérer vos données personnelles? / Which of the following actors do you trust the most to handle your personal data? 1) Entreprises privées / Private companies 2) Administrations publiques / Public service 3)Associations, fondations, etc. / NGOs, associations, foundations, etc 4) Aucun d'entre eux / None of the above

Poll Seed Statements:

We launched the poll with 15 seed statements. After approximately 1 month, we added 2 more seed statements on 18th July 2022.

S/N	Statement	Theme

1	Je crains pour ma sécurité physique dans les espaces publics (p. ex., les parcs et les rues) de Genève. / I fear for my physical security in the public spaces (e.g. parks and streets) of Geneva.	Physical Security
2	La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me.	Overwhelm from increased digitalisation
3	Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.	Digital Surveillance's influence on daily life
4	Je crains d'être victime d'escroqueries, de vols d'identité, de phishing et de fraudes financières. / I fear being a victim of scams, identity thefts, phishing and backing/financial frauds.	Victim of digital crimes
5	La plupart des gens ne signalent pas les crimes numériques (p. ex. le piratage ou le harcèlement en ligne). / Most people do not report digital crimes (e.g., being hacked, digital harassment).	Reporting of digital crimes
6	Les autorités genevoises sont bien équipées et compétentes pour protéger ma vie numérique. / The Geneva authorities are well equipped and competent to protect my digital life.	Competence of Geneva authorities
7	Je me sentirais plus en sécurité si la police et le gouvernement utilisaient davantage de technologies pour me protéger. / I would feel more secure if the police and the government used more technology to protect me.	Openness to police and government to use technologies for protection

8	Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.	Mis-use of data by Government
9	Je crains que les décisions concernant ma vie quotidienne (p.ex. travail, santé, logement) soient de plus en plus prises par des algorithmes. / I fear that decisions about my daily life (e.g., work, health, housing) are increasingly made by algorithms.	Algorithmic influence on daily life
10	Je crains que les grandes entreprises technologiques (ex. Facebook, Google) utilisent mes données sans que je m'en rende compte. / I fear that big tech companies (e.g. Facebook, Google) are using my data for purposes I am unaware of.	Awareness of use of data by Big Tech
11	Je crains que les données que les entreprises privées (ex. Facebook, Google) détiennent à mon sujet soient utilisées de manière inappropriée. / I fear that the data private companies have about me is improperly used.	Misuse of data by Big Tech
12	Les médias sociaux sont une source crédible d'informations et de nouvelles pour me tenir au courant des menaces de sécurité à Genève. / Social media is a reliable source of information and news to keep me aware of security threats in Geneva.	Credibility of social media
13	Partager des incidents sur les médias sociaux est plus efficace que de les signaler aux autorités. / Sharing incidents on social media is more effective than reporting it to the authorities.	Sharing incidents on social media

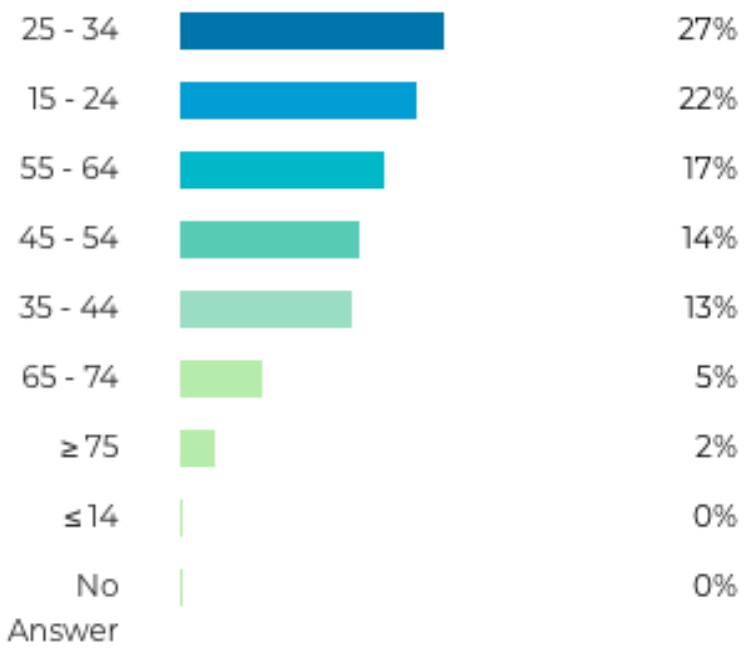
14	La dépendance aux technologies et la réduction de la durée d'attention ont créé un problème de santé publique. / Addiction to technologies and the reduction of attention spans has created a problem to public health.	Addiction and attention span on public health
15	Le processus d'accès et de remplissage des formulaires administratifs numériques de la ville et du canton est difficile pour moi. / The process of accessing and filling up digital city and cantonal administrative forms is difficult for me.	Digital admin forms
16	Je suis d'accord que mes données personnelles récoltées par les administrations publiques soient hébergées sur des serveurs à l'étranger. / I agree to have personal data collected by the government to be stored in servers outside Switzerland.	Storage of personal data in foreign servers
17	J'ai déjà envisagé ce scénario: des services numériques, utilisés quotidiennement, inaccessibles pendant une durée indéterminé. / I have already imagined a scenario where digital services that I use daily are unavailable for a period of time.	Interruptions in digital services

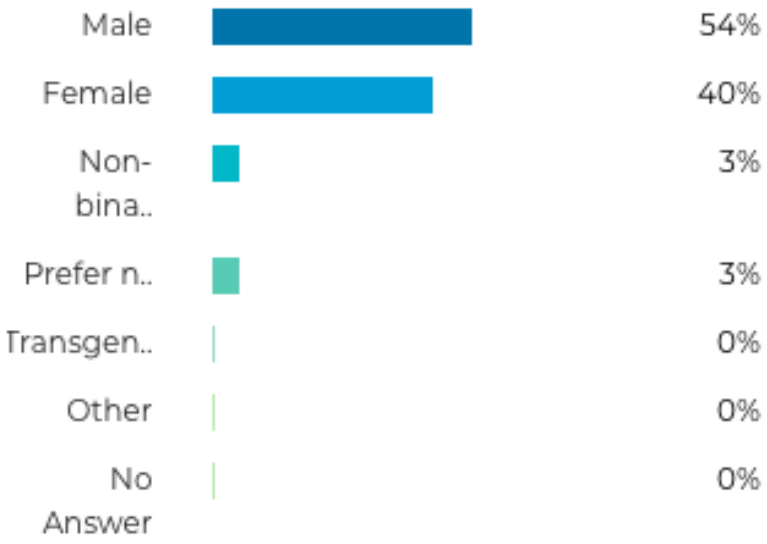
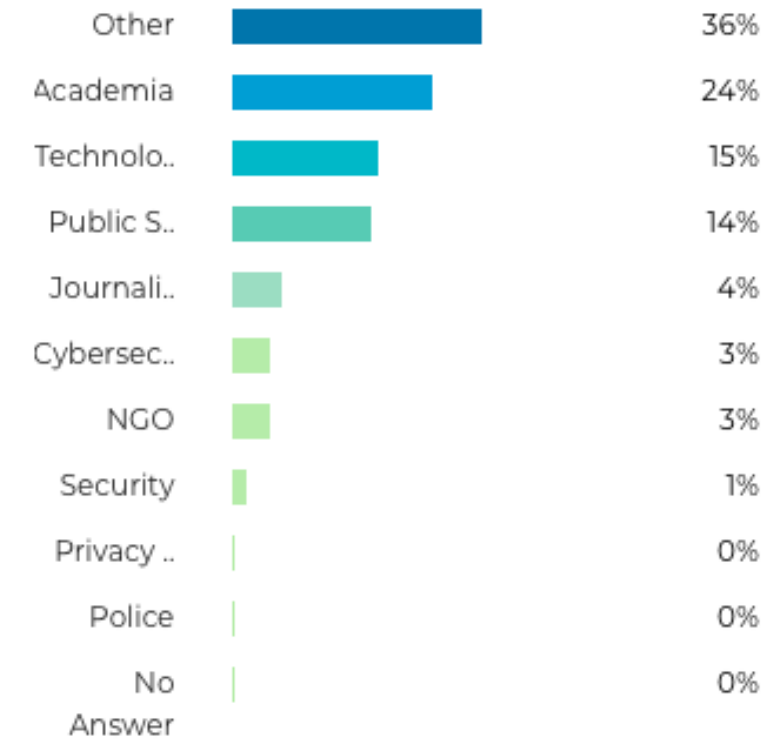
Poll Results

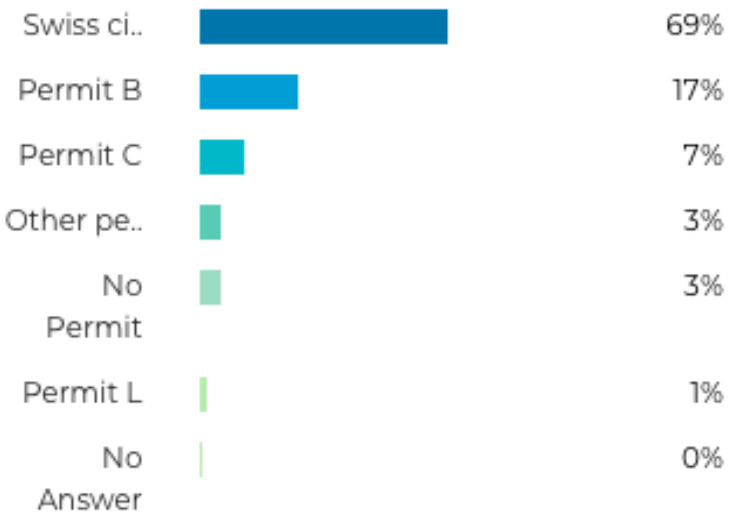
Headline Results:

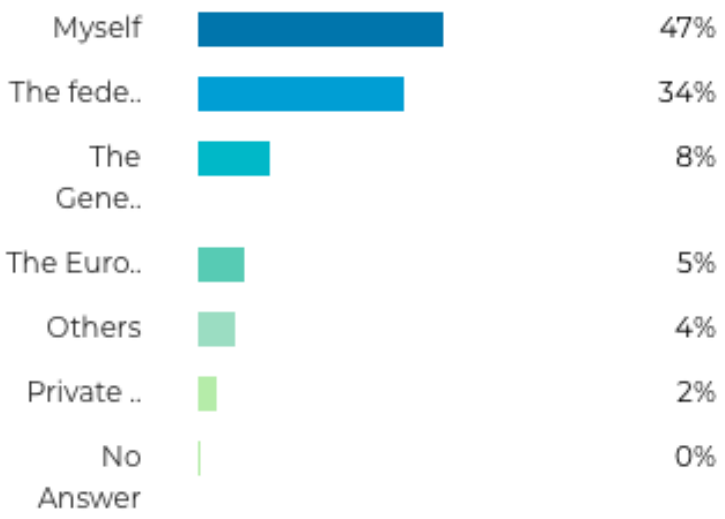
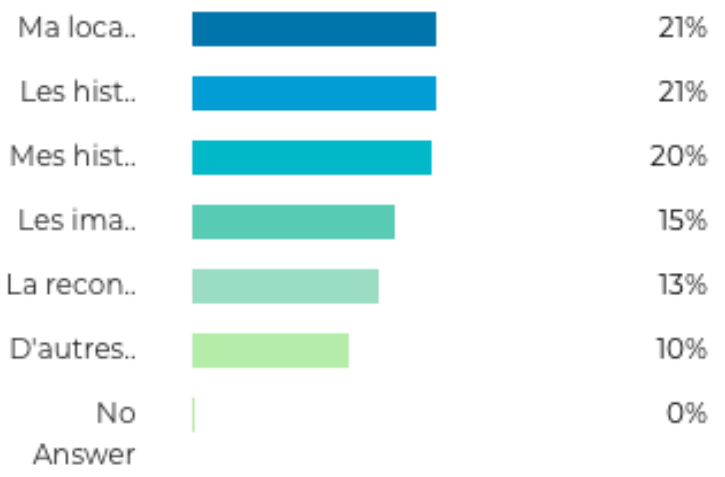
Total number of participants: 414
Number of participants who voted on 7 or more statements: 413
Number of votes cast across all 17 statements: 6,626
Seed statements: 15
Enabled statements: 2
Number of comments: 114

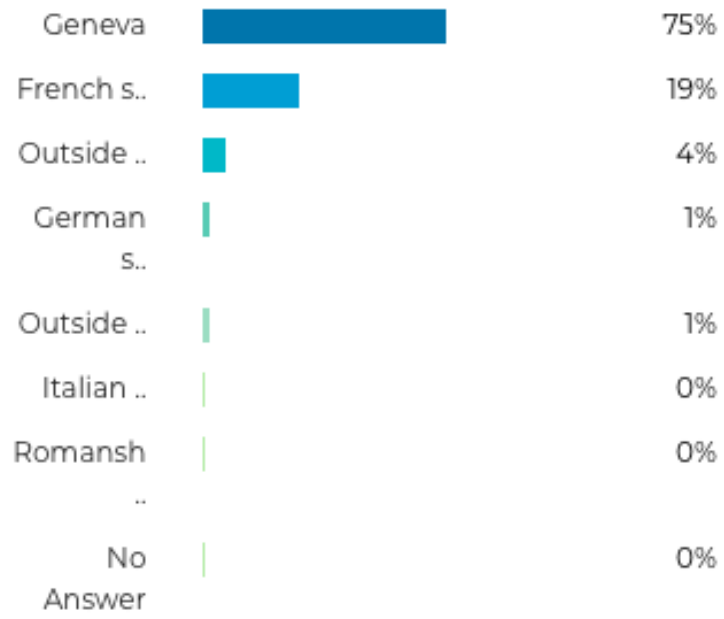
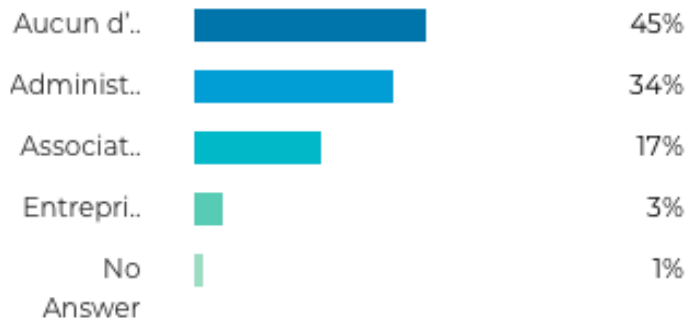
MCQs/Variables:

1. Age	How old are you? / Quel est votre âge ?  Based on the above results, we can discount the age-groups from 65 years old and above from any meaningful analysis due to their lack of representation.

2. Gender	What's your gender? / Quel est votre sexe ?  Based on the above results, we can discount all genders, except for male and female, from any meaningful analysis due to their lack of representation.
3. Occupation/Role	What's your sector? / Quel est votre secteur ? 

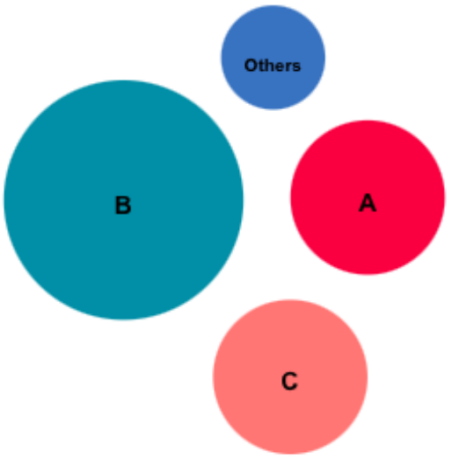
	Based on the above results, we should include only “other”, “academia”, “technology” and “public sector” for any meaningful analysis.
4. Citizenship/Migration Status	Which of the following best describes your residency status in Geneva? / Lequel des choix suivants vous décrit le mieux ?  Based on the above results, there is sufficient representation from Swiss citizens, Permit B holders and to a smaller extent, Permit C holders for any meaningful analysis. .
5. Responsibility	Which of the following should be mainly responsible for your digital security? / Laquelle des entités suivantes devrait avoir la principale responsabilité de ma sécurité numérique ?

	 Based on the above results, there is sufficient representation from 'Myself", "The Federal Government" and "The Geneva Authorities" for any meaningful analysis.
6. Perception of data being collected *Note: This was the only MCQ that allowed participants to choose more than 1 option	What kinds of data do you think is being collected about you? You may select more than 1 option. / Selon vous, quels types de données sont collectés sur vous et à votre sujet? Vous pouvez sélectionner plus d'une option.  It is interesting to note that the top 3 types of data that people think are being collected are location and browsing data and purchasing history. The next 3 are video footage, facial recognition and "others".

7. Location	Vous habitez où en ce moment? / Where do you currently live?  We are able to do meaningful analysis on Geneva residents and residents from the French speaking regions due to their sufficient representation in the responses.
8. Trusted Actors *Note: This MCQ was added	Parmi les acteurs suivants, auxquels faites-vous le plus confiance pour gérer vos données personnelles? / Which of the following actors do you trust the most to handle your personal data?  The three actors that are trusted the most are in the following descending order: “none of the above”, public services, and finally NGOS, associations and foundations.

Opinion Groups:

The OPPI algorithm analyses all votes and determines the landscape of opinions according to the voting patterns of the poll participants. OPPI clusters and discovers the various tribes based on how similar or different the respondents vote. Statements that uniquely express the sentiments of different tribes, personas or archetypes are identified by the algorithm. These OPPi opinion clusters simplify a leader's understanding of the "lay of the land" or the tribes that people fall under so that targeted communications, engagement or policy decisions can be formulated for different tribes. For our poll, the algorithm picked out 3 main opinion groups among the 414 respondents.



GROUP A
22%
of participants belongs to Group A

GROUP B
53%
of participants belongs to Group B

GROUP C
22%
of participants belongs to Group C

GROUP OTHERS
2%
of participants belongs to Group Others

Group	A (22%)	B (53%)	C (22%)
Persona / Archetype	Secure and Safe	Insecure and Afraid	Either Undecided or Afraid
Key Attributes	Unafraid, safe and secure	Fearful, unsafe and insecure	Undecided or insecure and afraid

Detailed Attributes	- Do not fear decisions about daily life are made by algorithms - Do not fear increased presence of digital surveillance - Do not fear improper use of personal data by Geneva government - Do not feel overwhelmed by increasing digitalization of urban and social life	- Fear increased presence of digital surveillance - Does not feel secure if police and government used technology to protect me - Fear improper use of personal data by Geneva government - Overwhelmed by increasing digitalization of urban and social life - Does not feel that Geneva authorities are well equipped to protect my digital life	- Undecided or fearful that decisions about daily life are made by algorithms - Undecided or fearful of increased presence of digital surveillance - Undecided or unfearful about improper use of personal data by Geneva government - Undecided or disagree on difficulty of filling up digital admin forms - Undecided or disagree on personal data by government being stored overseas

Here are the statements that uniquely identify each of the 3 opinion groups.

5 statements that are unique to Group A

9 3 8 2 17

Je crains que les décisions concernant ma vie quotidienne (p.ex. travail, santé, logement) soient de plus en plus prises par des algorithmes. / I fear that decisions about my daily life (e.g., work, health, housing) are increasingly made by algorithms.

47% of participants in group A **disagreed** on **statement 9**

Agree Disagree Undecided Pass / Unseen

Group A	43% 47% 10%	Group B	92% 4% 5%
Group C	54% 16% 30%	Group Others	29% 57% 14%

9 3 8 2 17

Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.

65% of participants in group A **disagreed** on **statement 3**

Agree Disagree Undecided Pass / Unseen

Group A	33% 65% 2%	Group B	94% 3% 3%
Group C	38% 20% 41%	Group Others	29% 43% 29%

9 3 8 2 17

Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.

74% of participants in group A **disagreed** on **statement 8**

Agree Disagree Undecided Pass / Unseen

Group A	24% 74% 1%	Group B	73% 14% 13%
Group C	15% 29% 55%	Group Others	0% 57% 43%

9 3 8 2 17

La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me.

83% of participants in group A **disagreed** on **statement 2**

Agree Disagree Undecided Pass / Unseen

Group A	9% 83% 9%	Group B	68% 18% 14%
Group C	17% 44% 39%	Group Others	0% 57% 43%

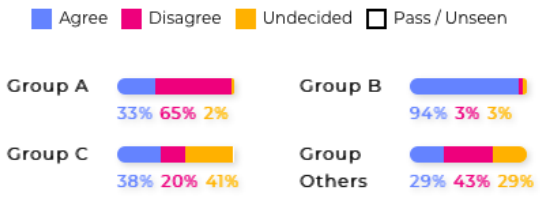
9 3 8 2 17 **J'ai déjà envisagé ce scénario: des services numériques, utilisés quotidiennement, inaccessibles pendant une durée indéterminé. / I have already imagined a scenario where digital services that I use daily are unavailable for a period of time.**   30% of participants in group A **disagreed** on **statement 17** Agree Disagree Undecided Pass / Unseen Group A 37% 30% 1% Group B 44% 2% 4% Group C 32% 4% 22% Group Others 0% 29% 43%	

5 statements that are unique to Group B

3 7 8 2 6

Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.

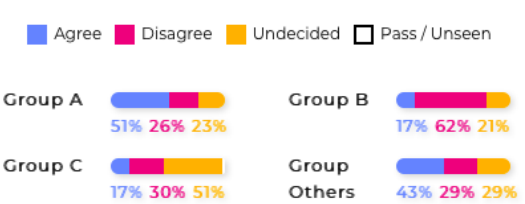
94% of participants in group B **agreed** on **statement 3**



3 7 8 2 6

Je me sentirais plus en sécurité si la police et le gouvernement utilisaient davantage de technologies pour me protéger. / I would feel more secure if the police and the government used more technology to protect me.

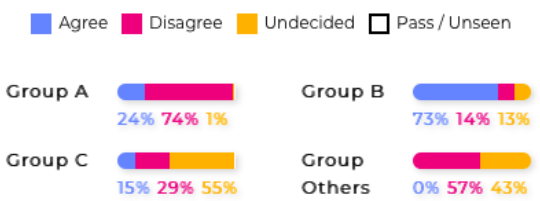
62% of participants in group B **disagreed** on **statement 7**



3 7 8 2 6

Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.

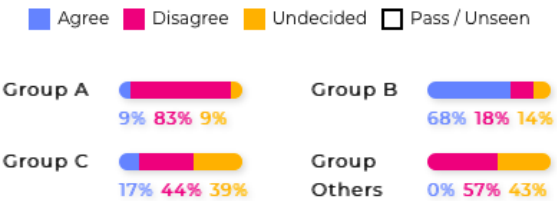
73% of participants in group B **agreed** on **statement 8**



3 7 8 2 6

La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me.

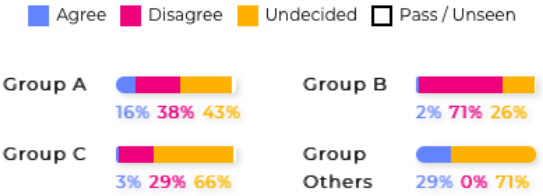
68% of participants in group B **agreed** on **statement 2**



3 7 8 2 6

Les autorités genevoises sont bien équipées et compétentes pour protéger ma vie numérique. / The Geneva authorities are well equipped and competent to protect my digital life.

71% of participants in group B **disagreed** on **statement 6**

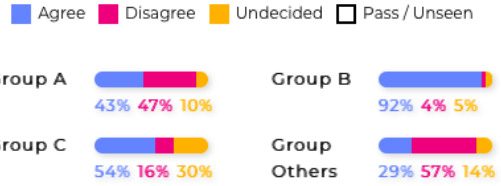


5 statements that are unique to Group C

9 3 8 15 16

Je crains que les décisions concernant ma vie quotidienne (p.ex. travail, santé, logement) soient de plus en plus prises par des algorithmes. / I fear that decisions about my daily life (e.g., work, health, housing) are increasingly made by algorithms.

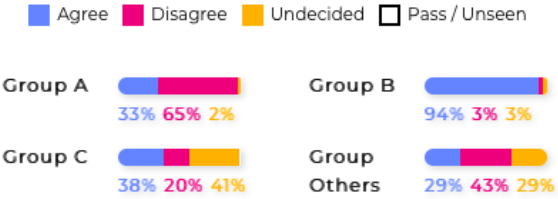
30% of participants in group C undecided on **statement 9**



9 3 8 15 16

Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.

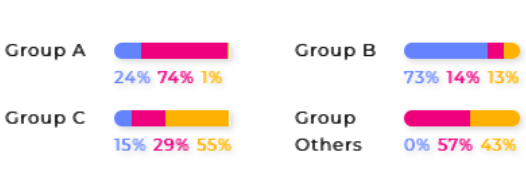
41% of participants in group C undecided on **statement 3**



9 3 8 15 16

Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.

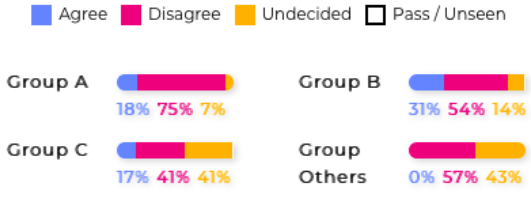
55% of participants in group C undecided on **statement 8**

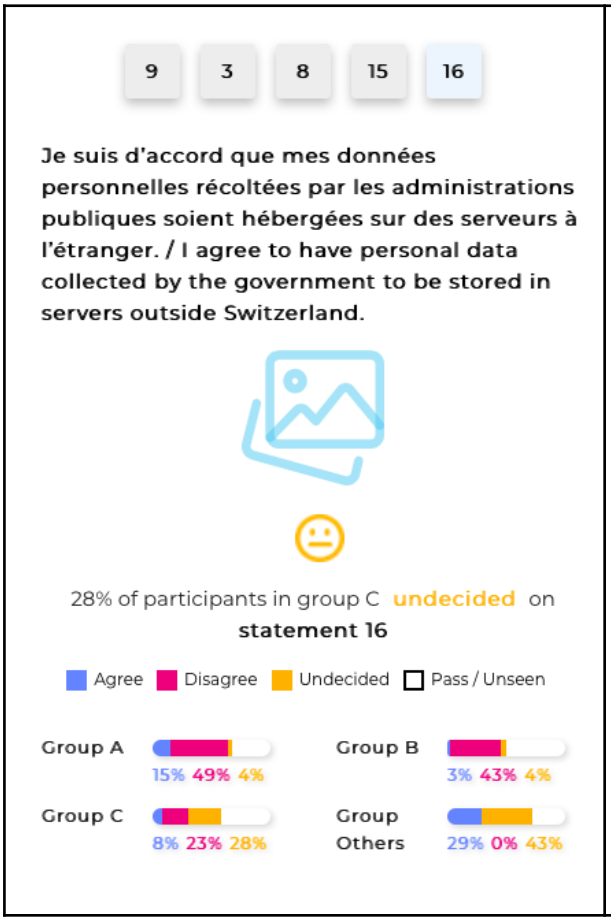


9 3 8 15 16

Le processus d'accès et de remplissage des formulaires administratifs numériques de la ville et du canton est difficile pour moi. / The process of accessing and filling up digital city and cantonal administrative forms is difficult for me.

41% of participants in group C undecided on **statement 15**





Decision Matrix (DM):

OPPi's decision-matrix (or So-What Chart) converts all statements into bubbles onto a visual plane, thus giving us a "bird's eye or helicopter view" of the discussion. The decision matrix allows key decision-makers to do three things:

a. Structure and design their next course of action and follow-up engagement sessions (e.g. focus group discussions and physical townhalls) according to the five buckets or categories.
b. Allocate resources (time, energy and money) optimally across the five buckets/categories.
c. Monitor the evolution of the issues and adjust strategies accordingly in real-time.

The ultimate goal of the DM is to help an organisation or society keep track of the "hot-button" and difficult issues and measure their progress over time. Beyond a progress-tracker, OPPi's DM gamifies the entire process of consensus-building for all members of an organisation and society. More information on the DM can be found in the following medium article written by Santosh, founder of Soul Probe: https://medium.com/your-oppi/oppis-decision-matrix-41d96f332878

There are two axes to the DM. The x-axis is the Consensus Factor while the y-axis is the Participation Factor. The size of the bubble is correlated to the Certainty Factor.

Consensus Factor = |No. of Agrees — No. of Disagrees| / (No. of Agrees + No. of Disagrees + No. of Undecideds)

Participation Factor = (No. of Agrees + No. of Disagrees + No. of Undecideds) / Total no. of Participants (i.e. both active and non-active participants)

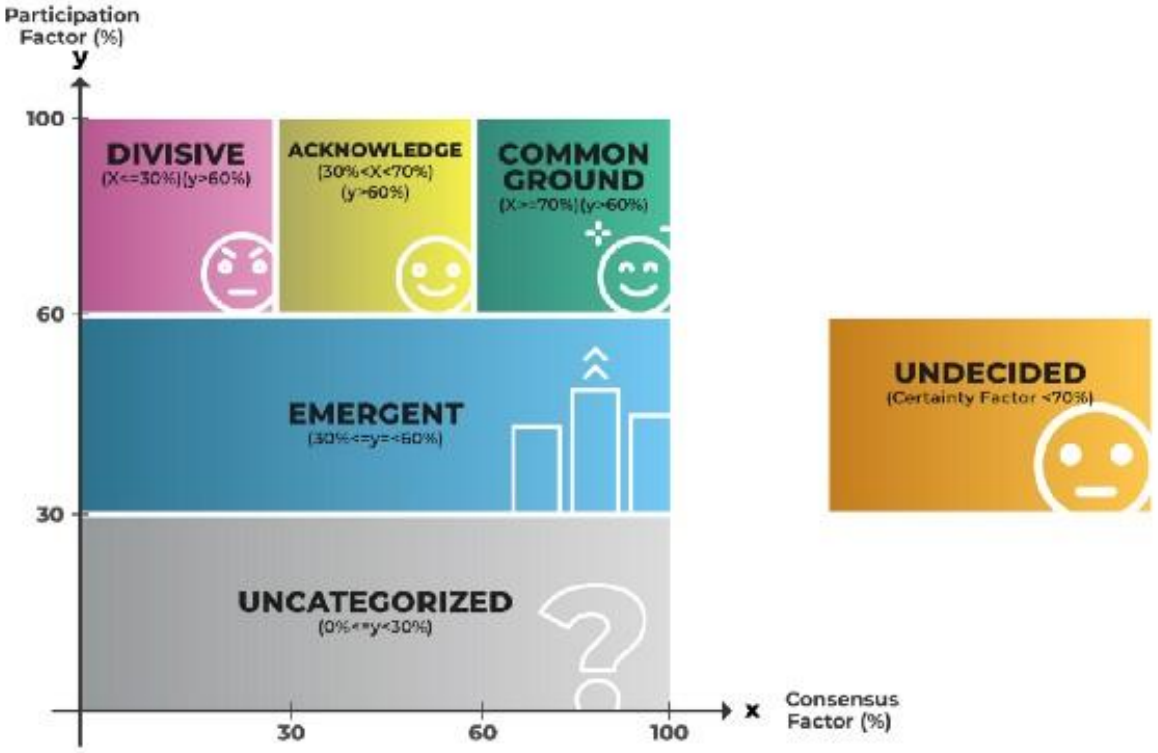
Certainty Factor = 1 — [No. of Undecideds / (No. of Agrees + No. of Disagrees + No. of Undecideds)]

Consensus Factor shows how much participants actually agree or disagree with a statement that they have seen. The higher the consensus, the greater the amount of agree-ness or disagree-ness from the participants.

In OPPi, certain statements are crowdsourced from the participants, so naturally, not all participants may have seen every statement. Participation Factor indicates how many of the participants have voted on the statements. To increase the participation factor on a statement, organisers can consider re-inviting the participants to vote on new statements whenever they are available.

Certainty Factor refers to the amount of certainty that participants expressed in agreeing or disagreeing with a statement.

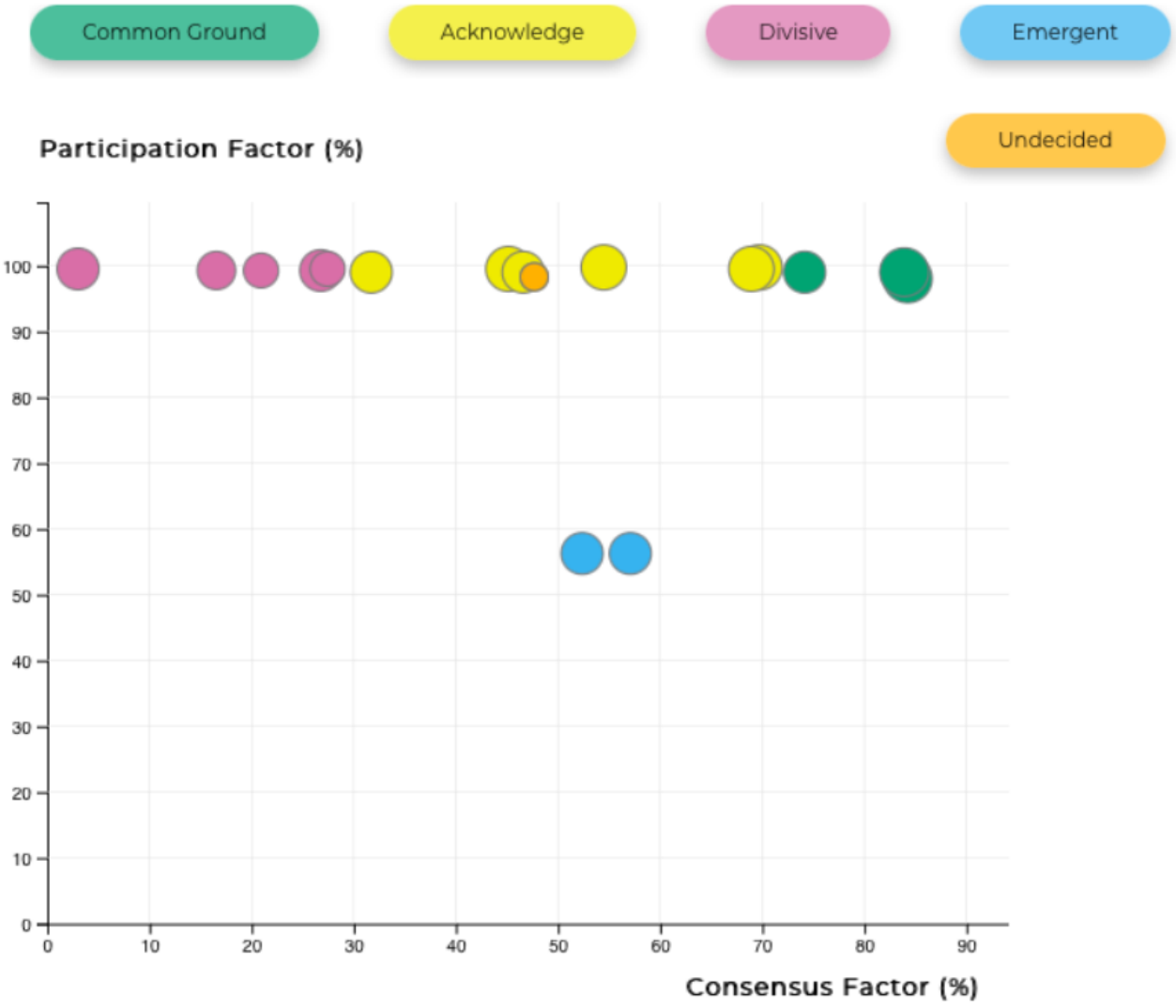
Statements and opinions in the OPPi conversation are classified into six distinct categories as depicted in the diagram below:



Six categories of the Decision Matrix. All except for Undecided are mutually exclusive categories.

The six categories offer poll organisers insights on how they can interpret the voting patterns of the participants.

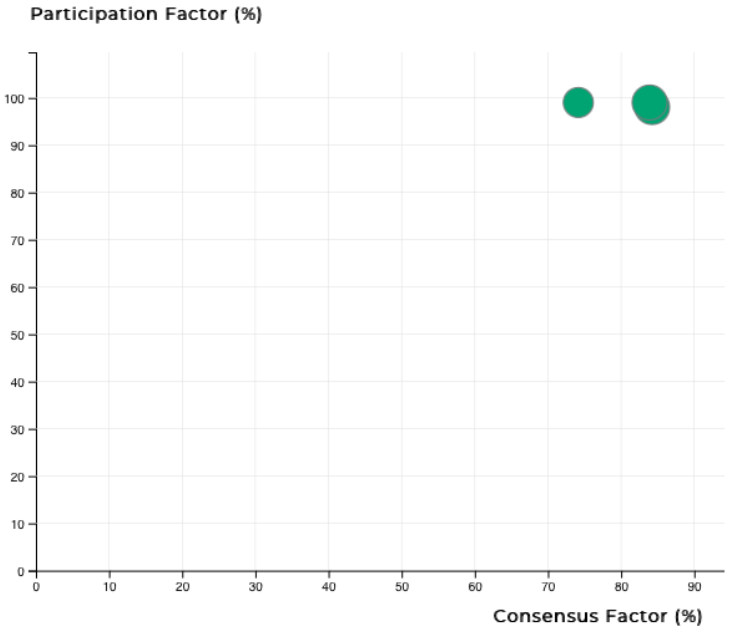
For our poll, the 17 statements were classified under 5 distinct categories as shown in the diagram below.



3 Common Ground Statements (In Green)

EDGELANDS institute

Common Ground | Acknowledge | Divisive | Emergent | Undecided



11 Je crains que les données que les entreprises privées (ex. Facebook, Google) détiennent à mon sujet soient utilisées de manière inappropriée. / I fear that the data private companies have about me is improperly used.

89.27% Agree | 5.37% Disagree | 5.37% Undecided | 410 Votes

10 Je crains que les grandes entreprises technologiques (ex. Facebook, Google) utilisent mes données sans que je m'en rende compte. / I fear that big tech companies (e.g. Facebook, Google) are using my data for purposes I am unaware of.

89.66% Agree | 5.42% Disagree | 4.93% Undecided | 406 Votes

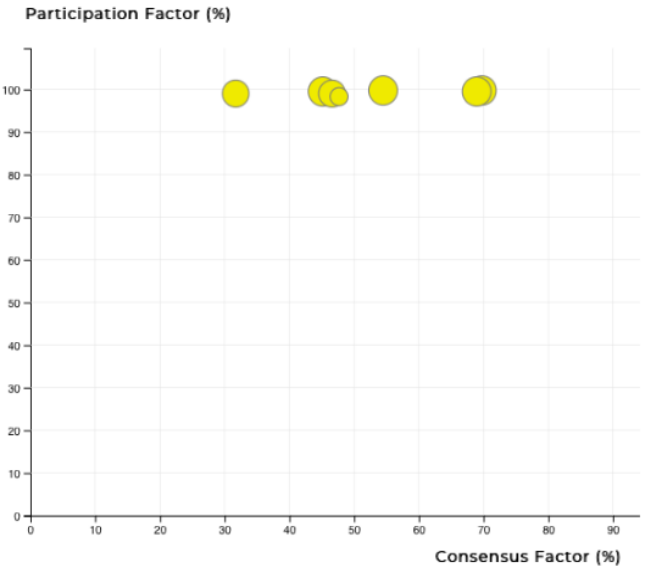
5 La plupart des gens ne signalent pas les crimes numériques (p. ex. le piratage ou le harcèlement en ligne). / Most people do not report digital crimes (e.g., being hacked, digital harassment).

79.27% Agree | 5.12% Disagree | 15.61% Undecided | 410 Votes

7 Acknowledge Statements (In Yellow)

EDGELANDS institute

Common Ground | Acknowledge | Divisive | Emergent | Undecided



1 Je crains pour ma sécurité physique dans les espaces publics (p. ex., les parcs et les rues) de Genève. / I fear for my physical security in the public spaces (e.g. parks and streets) of Geneva.

10.19% Agree | 79.13% Disagree | 10.68% Undecided | 412 Votes

3 Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.

66.75% Agree | 21.6% Disagree | 11.65% Undecided | 412 Votes

6 Les autorités genevoises sont bien équipées et compétentes pour protéger ma vie numérique. / The Geneva authorities are well equipped and competent to protect my digital life.

6.14% Agree | 53.81% Disagree | 40.05% Undecided | 407 Votes

9 Je crains que les décisions concernant ma vie quotidienne (p.ex. travail, santé, logement) soient de plus en plus prises par des algorithmes. / I fear that decisions about my daily life (e.g., work,

71.43% Agree | 16.95% Disagree | 11.62% Undecided | 413 Votes

12 Les médias sociaux sont une source crédible d'informations et de nouvelles pour me tenir au courant des menaces de sécurité à Genève. / Social media is a reliable source of information and news to keep me aware of security threats in Geneva.

16.83% Agree | 63.41% Disagree | 19.76% Undecided | 410 Votes

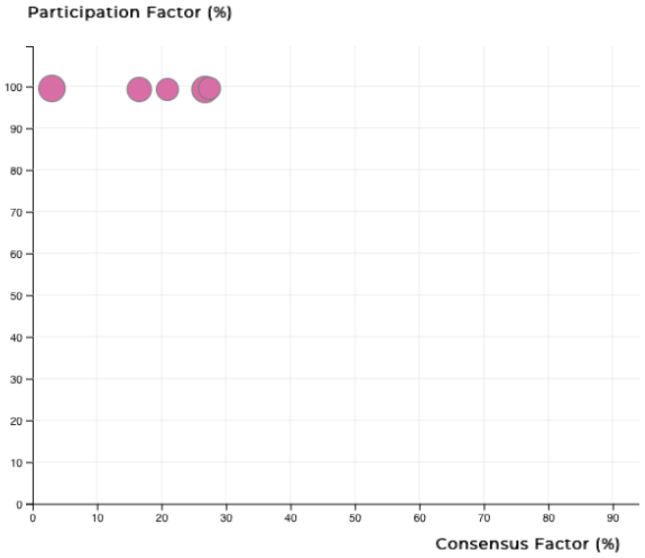
14 La dépendance aux technologies et la réduction de la durée d'attention ont créé un problème de santé publique. / Addiction to technologies and the reduction of attention spans has created a problem to public health.

78.69% Agree | 8.96% Disagree | 12.35% Undecided | 413 Votes

15 Le processus d'accès et de remplissage des formulaires administratifs numériques de la ville et du canton est difficile pour moi. / The process of accessing and filling up digital city and cantonal administrative forms is difficult for me.

24.63% Agree | 56.34% Disagree | 19.02% Undecided | 410 Votes

5 Divisive Statements (In Red)



13 Partager des incidents sur les médias sociaux est plus efficace que de les signaler aux autorités. / Sharing incidents on social media is more effective than reporting it to the authorities.

21.84% Agree | 49.27% Disagree | 28.88% Undecided | 412 Votes

2 La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me.

42.23% Agree | 38.83% Disagree | 18.93% Undecided | 412 Votes

8 Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.

48.18% Agree | 31.63% Disagree | 20.19% Undecided | 411 Votes

7 Je me sentirais plus en sécurité si la police et le gouvernement utilisaient davantage de technologies pour me protéger. / I would feel more secure if the police and the government used more technology to protect me.

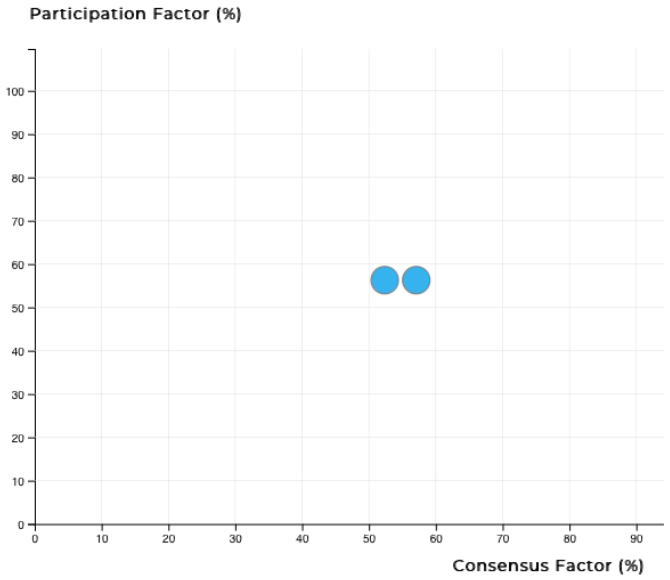
25.3% Agree | 46.23% Disagree | 28.47% Undecided | 411 Votes

4 Je crains d'être victime d'escroqueries, de vols d'identité, de phishing et de fraudes financières. /

55.23% Agree | 28.47% Disagree | 16.3% Undecided | 411 Votes

2 Emergent Statements (in Blue)

Common Ground | Acknowledge | Divisive | **Emergent** | Undecided



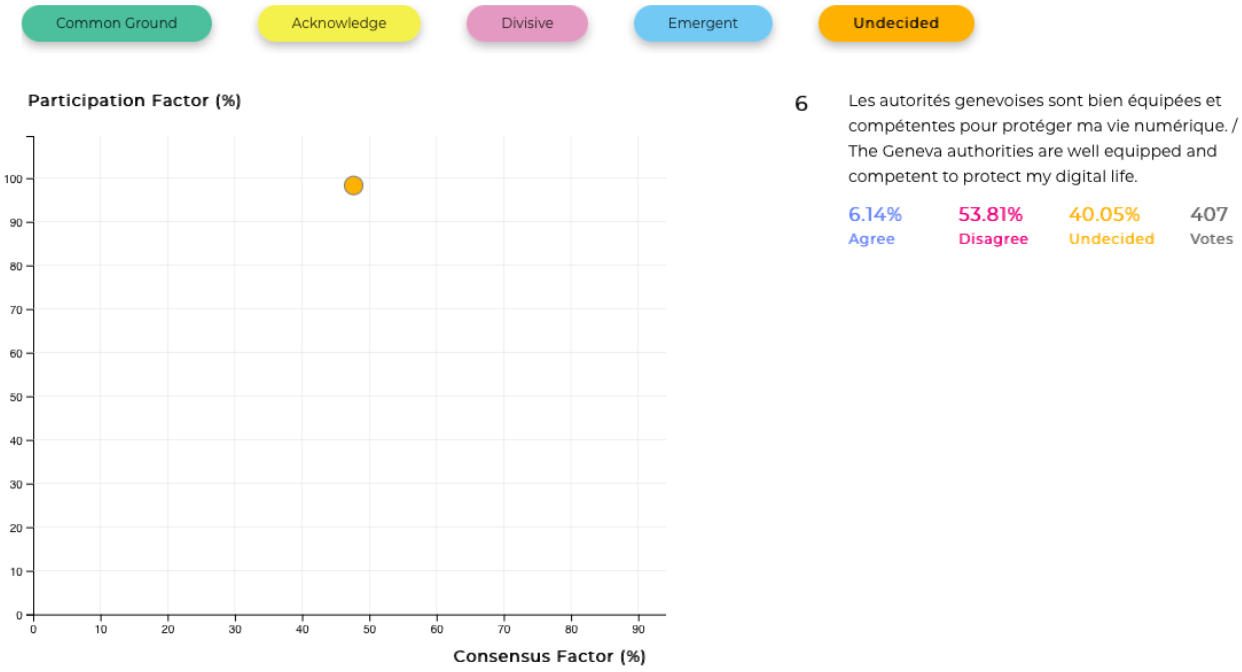
16 Je suis d'accord que mes données personnelles récoltées par les administrations publiques soient hébergées sur des serveurs à l'étranger. / I agree to have personal data collected by the government to be stored in servers outside Switzerland.

12.45% Agree | 69.53% Disagree | 18.03% Undecided | 233 Votes

17 J'ai déjà envisagé ce scénario: des services numériques, utilisés quotidiennement, inaccessibles pendant une durée indéterminé. / I have already imagined a scenario where digital services that I use daily are unavailable for a period of time.

69.1% Agree | 16.74% Disagree | 14.16% Undecided | 233 Votes

1 Undecided Statement (in Orange)



'Axis of Fear' and 'Axis of Agreement":

7 statements out of 17 statements measured sentiments on respondents' fears on a range of issues. We ranked the fears of these 7 issues and created a hypothetical 'Axis of Fear' as follows.

Fear of or lack of	Physical Security	Improper use of personal data by Government	Victim of digital frauds	Increased digital surveillance in daily life	Decisions on daily life being made by algorithms	Unknown/ unaware use of personal data by big tech	Improper use of personal data by Big Tech
Percentage of respondents in ascending order	10%	48%	55%	66%	71%	88%	88%

From the table above, we can see that the fears of use of personal data by big tech were the highest, followed by algorithms, then surveillance, then digital frauds,

then improper use of personal data by the government and lastly the fear of physical security.

For the remaining 10 statements which were not fear related, we created another 'Axis of Agreement' to rank these issues according to the percentage agreement they garnered from the respondents. This 'Axis of Agreement' can also be called an 'Axis of Public Approval or Confidence'.

Issue	Competence of authorities to protect digital life	Personal data collected by government to be stored in overseas servers	Reliability of social media to keep me aware of security threats in Geneva	Effectiveness of sharing incidents on social media as compared to reporting to the authorities	Difficulty in accessing and filling up digital government forms	Feel more secure if authorities used more tech to protect me	Increased digitalisation of urban and social life being overwhelming	Envisaged possibility that digital services are not available	Perception of people in Geneva not reporting digital crimes to the authorities	Addiction to devices and reduction in attention spans having created a problem for public health
Percentage agreement in ascending order	6%	12%	17%	22%	24%	25%	42%	69%	79%	79%

From the table below we can see that trust in the competence of authorities to protect digital life was the lowest, followed by trust in reliability of and effectiveness of social media and then feelings of security with authorities using more technology to protect citizens.

Addiction and attention span contributing to a problem for public health registered the highest agreement followed by the perception of people in Geneva reporting digital crimes, the possibility of envisaging a digital service 'outage',

then the overwhelm from digitalisation of urban and social life, the difficulty of digital government forms and finally agreeing that personal data collected by government be stored overseas.

Insights on Consensus Factor for each statement:

S/N	Statement	Theme	Insight
1	Je crains pour ma sécurité physique dans les espaces publics (p. ex., les parcs et les rues) de Genève. / I fear for my physical security in the public spaces (e.g. parks and streets) of Geneva.	Physical Security	A high majority (79%) of the respondents did not fear for their physical security. This statement had the 4th highest consensus factor among all 17 statements at 68.93%.
2	La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me.	Overwhelm from increased digitalisation	Respondents in the poll were the most divided about this statement among all 17 statements with the lowest consensus factor of 3.4%.
3	Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.	Digital Surveillance's influence on daily life	In contrast to physical security (statement 1), a majority of respondents (66.75%) fear the increased presence of digital surveillance in their lives. The consensus was significantly lower than statement 1 at 45.2%, meaning there was a significant or non-negligeable 21.6% that did not fear the increased presence of digital surveillance.

4	Je crains d'être victime d'escroqueries, de vols d'identité, de phishing et de fraudes financières. / I fear being a victim of scams, identity thefts, phishing and backing/financial frauds.	Victim of digital crimes	In contrast to the high consensus factor for physical security, respondents' sentiments on being digital victims was the 4th most divisive statement among all 17 statements with a very low consensus factor of 26.76%.
5	La plupart des gens ne signalent pas les crimes numériques (p. ex. le piratage ou le harcèlement en ligne). / Most people do not report digital crimes (e.g., being hacked, digital harassment).	Reporting of digital crimes	This statement had the 3rd highest agreement (79.27%) among all 17 statements. This statement also had the 3rd highest consensus factor among all the 17 statements in the poll indicating a social norm that is widely pervasive and ingrained in the citizens of Geneva about the issue.
6	Les autorités genevoises sont bien équipées et compétentes pour protéger ma vie numérique. / The Geneva authorities are well equipped and competent to protect my digital life.	Competence of Geneva authorities	Most of the respondents (93.85%) either disagreed (53.8%) or were undecided (40.05%) on the competence of the authorities which indicated a high amount of mistrust by the respondents. Additionally, this was the statement that participants were most undecided about among all 17 statements. This indicates a strong need for the authorities to either strengthen its security capabilities and efforts, or earn the trust of or educate the public about its efforts to protect the digital lives of its citizens.
7	Je me sentirais plus en sécurité si la police et le gouvernement utilisaient davantage de technologies pour me protéger. / I would	Openness to police and government to use technolog	These 2 statements related to the police and government were the 2nd and 3rd most divisive statements among the 17 statements. This is in sharp contrast to the 2 statements (statements 10 and 11) on big tech companies which received

	feel more secure if the police and the government used more technology to protect me.	ies for protection	the highest consensus among the public. Statement 8 had a consensus factor of 16.6% while that of statement 7 was 20.9%. This high polarisation could indicate either: a. a lack of or differing levels of knowledge, understanding or education of the issue or b. mixed opinions about the issue or c. the lack of enough public debate and conversations that needed to be had on the issue.
8	Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.	Mis-use of data by Governme nt	
9	Je crains que les décisions concernant ma vie quotidienne (p.ex. travail, santé, logement) soient de plus en plus prises par des algorithmes. / I fear that decisions about my daily life (e.g., work, health, housing) are increasingly made by algorithms.	Algorithmi c influence on daily life	This statement had the 5th highest agreement (71.43%) among all 17 statements. It had a slightly lower consensus factor of 54.5%. The fear of algorithms was the 3rd biggest fear after the first two fears of big tech.
10	Je crains que les grandes entreprises technologiques (ex. Facebook, Google) utilisent mes données sans que je m'en rende compte. / I fear that big tech companies (e.g. Facebook, Google) are using my data for	Awarenes s of use of data by Big Tech	These 2 statements on the use of personal data by big tech companies had the highest consensus factor among all the 17 statements in the poll with 84.2% for statement 10 and 83.9% for statement 11. This possibly reflected a strong public awareness, sensitization, exposure, fear or support for the issue.

	purposes I am unaware of.		
11	Je crains que les données que les entreprises privées (ex. Facebook, Google) détiennent à mon sujet soient utilisées de manière inappropriée. / I fear that the data private companies have about me is improperly used.	Misuse of data by Big Tech	
12	Les médias sociaux sont une source crédible d'informations et de nouvelles pour me tenir au courant des menaces de sécurité à Genève. / Social media is a reliable source of information and news to keep me aware of security threats in Geneva.	Credibility of social media	63.4% of respondents disagreed that social media was a reliable source for security threats with a consensus factor of 46.6%, thus placing it in the "Acknowledge" category.
13	Partager des incidents sur les médias sociaux est plus efficace que de les signaler aux autorités. / Sharing incidents on social media is more effective than reporting it to the authorities.	Sharing incidents on social media	49.27% of respondents disagreed with the statement with 21.8% agreeing and 28.9% being undecided. It was the 2nd most undecided statement among the 17 statements. The statement was also the 5th most divisive statement among all 17 statements with a consensus of 27.4%.
14	La dépendance aux technologies et la réduction de la durée d'attention ont créé un	Addiction and attention span on	This statement, categorised in the "Acknowledge" category, registered the 4th highest agreement (78.69%) among all 17 statements. It had also the 4th

	problème de santé publique. / Addiction to technologies and the reduction of attention spans has created a problem to public health.	public health	highest consensus factor (69.7%) among all 17 statements which could have easily placed it in the “Common Ground” category like statements 5, 10 and 11.
15	Le processus d'accès et de remplissage des formulaires administratifs numériques de la ville et du canton est difficile pour moi. / The process of accessing and filling up digital city and cantonal administrative forms is difficult for me.	Digital admin forms	56.34% of respondents disagreed with the statement with 25.6% agreeing and 19.0% being undecided. It had a low consensus of 31.7% which made it the 6th most divisive statement among all 17 statements.
16	Je suis d’accord que mes données personnelles récoltées par les administrations publiques soient hébergées sur des serveurs à l’étranger. / I agree to have personal data collected by the government to be stored in servers outside Switzerland.	Storage of personal data in foreign servers	A significant 69.5% of respondents disagreed with the statement. The statement had a consensus of 57.1%.
17	J’ai déjà envisagé ce scénario: des services numériques, utilisés quotidiennement, inaccessibles pendant une durée indéterminé. / I have already imagined a scenario where digital	Interruptions in digital services	This statement registered the 6th highest agreement (69.1%) among all 17 statements. But it had a lower consensus factor of 52.36%

	services that I use daily are unavailable for a period of time.		

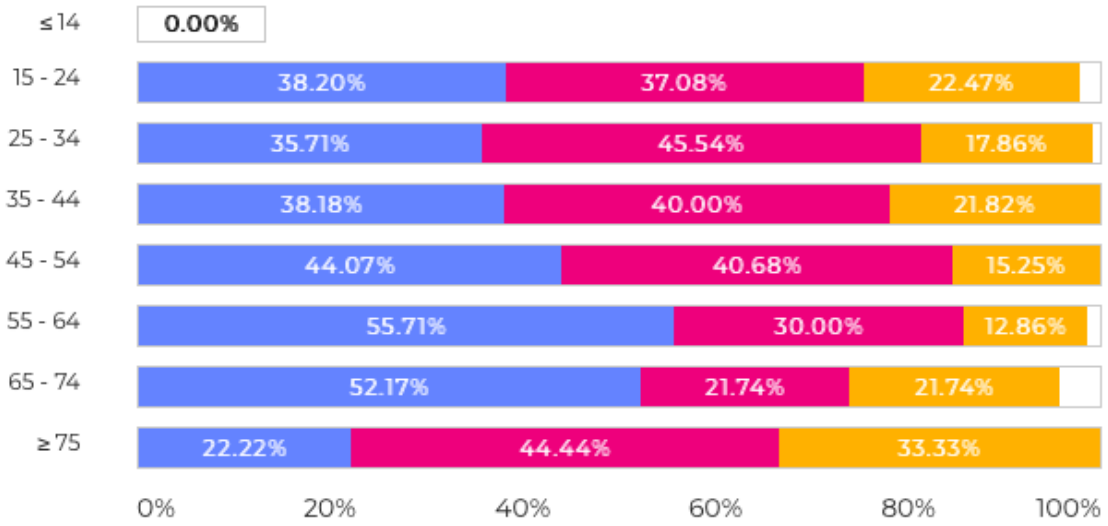
Salient MCQ Slide-and-Dice insights for key statements:

Statements with lower consensus factor became prime targets for deeper analysis for us to sieve out demographic differences in opinion which could have been possible causes for the division, rift or sway in public sentiments. Here are 7 key statements which had salient insights that were worth highlighting.

Statement 2:

"La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me."

Insight 1: There is a general trend line whereby the older the participants, the greater their overwhelm from the increased digitalization of urban and social life.

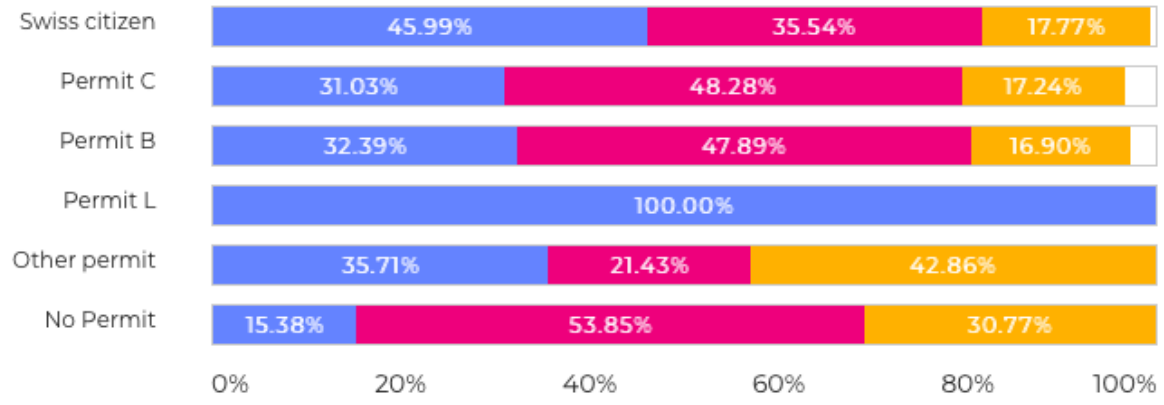


Insight 2: There was a significantly greater proportion (of around 15%) of Swiss citizens who felt overwhelmed as compared to Permit B and Permit C holders. The

other permit holders were not sufficiently represented in the sample for us to draw any meaningful conclusions.

Interestingly about 15% more Swiss citizens also feared the increased presence of digital surveillance in their daily life as compared to Permit B and C holders (statement 3).

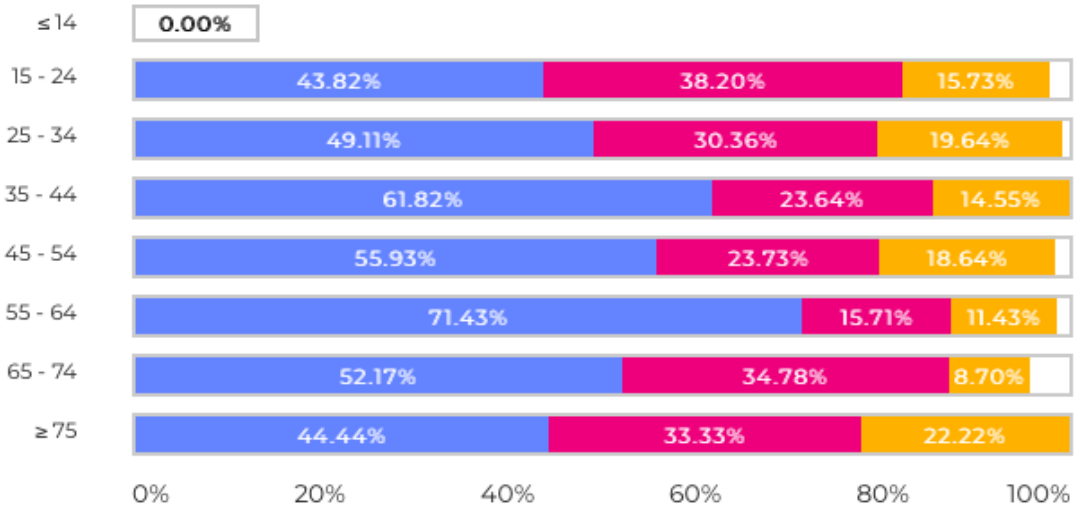
Note that Permit L and other options were discounted from the analysis due to the lack of sufficient representation.



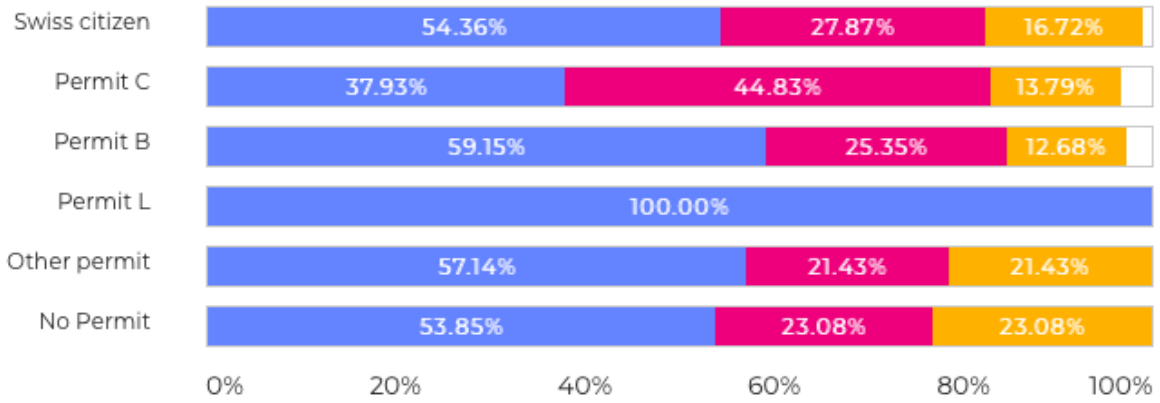
Statement 4:

"Je crains d'être victime d'escroqueries, de vols d'identité, de phishing et de fraudes financières. / I fear being a victim of scams, identity thefts, phishing and backing/financial frauds."

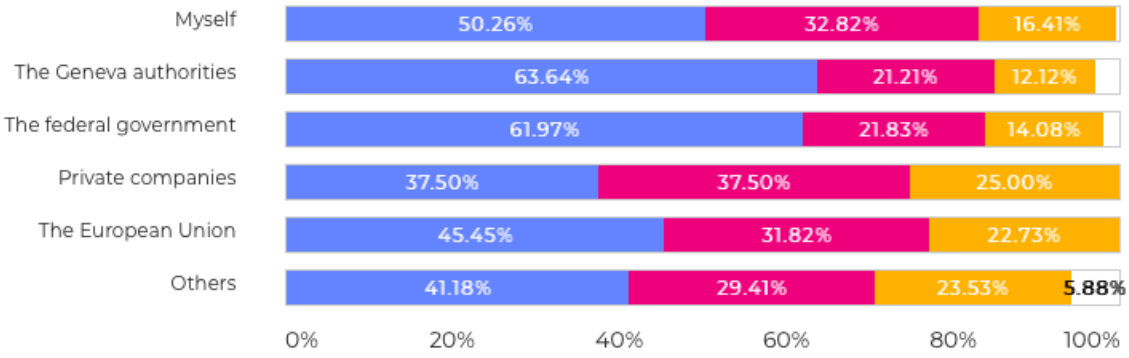
Insight 1: The elderly of age 55-64 expressed the greatest fear followed by a much younger age group of 35-44 and then 45-54 and then 65-74. The younger age group of 35-44 expressed greater fear possibly because the potential impact of loss could be higher due to their greater household and family responsibilities and commitments in life.



Insight 2: Swiss citizens and Permit B holders were more likely to fear being a victim of digital frauds.



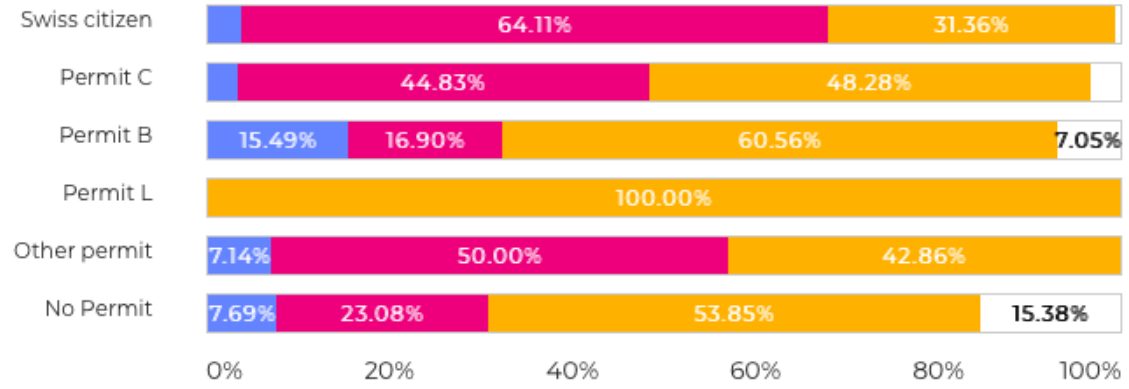
Insight 3: Those who indicated “Geneva authorities” and “Federal government” as being responsible for their digital security tend to have more fear of being a victim of digital fraud as compared to those who felt they themselves should be responsible. This seems to suggest that abdication of responsibility for one’s digital security could be correlated with one’s fear of being a digital fraud. It is important for us to stress that this insight is a correlation and not as a causation.



Statement 6:

“Les autorités genevoises sont bien équipées et compétentes pour protéger ma vie numérique. / The Geneva authorities are well equipped and competent to protect my digital life.”

Insight 1: A significantly greater proportion of Swiss citizens disagreed about the competence of the Geneva authorities as compared to Permit C holders. A disproportionately very high number of Permit B holders were undecided.

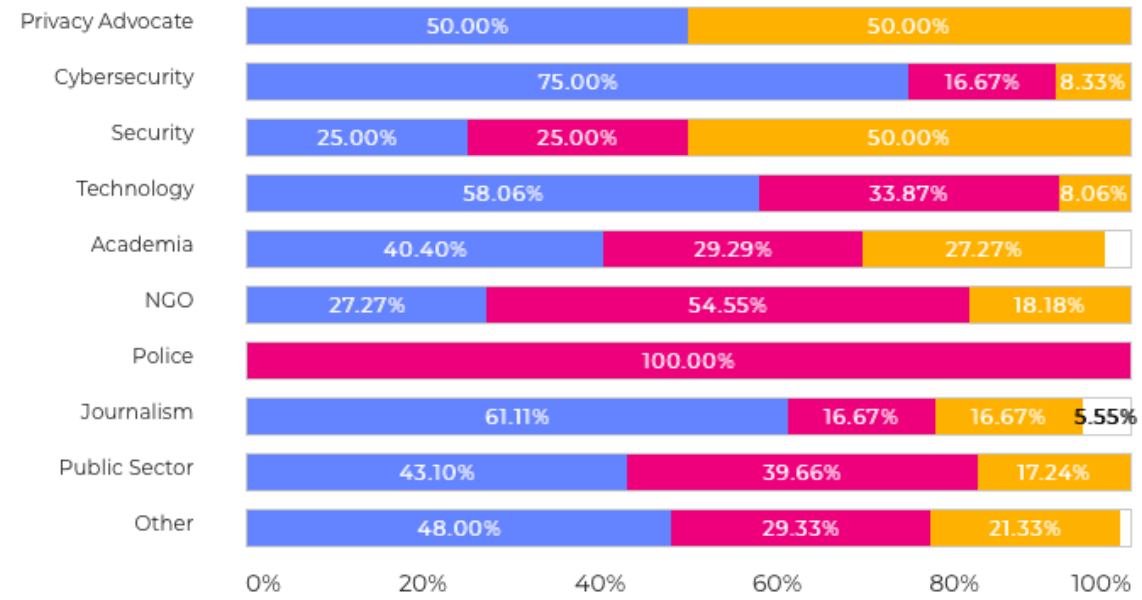


Statement 8:

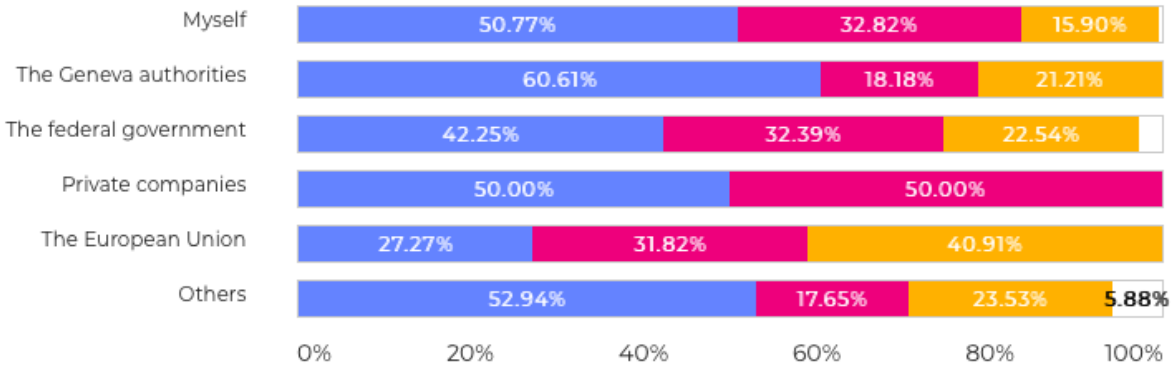
“Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.”

Insight 1: Only the following sectors of respondents were sufficiently representative for us to do meaningful analysis: “Other”, “Technology”, “Academia” and “Public Sector”. Among these 4 sectors, at least 10% more among those

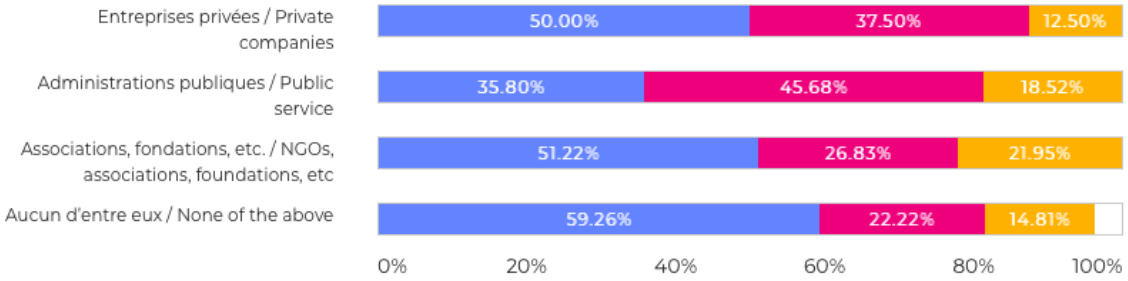
working in the tech sector agreed on this fear as compared to the percentage of those who agreed in the other 3 sectors.



Insight 2: Those who felt that the Geneva authorities should be responsible for their digital security tend to agree more on the fear as compared to those who felt that either the Federal government or themselves should be responsible.



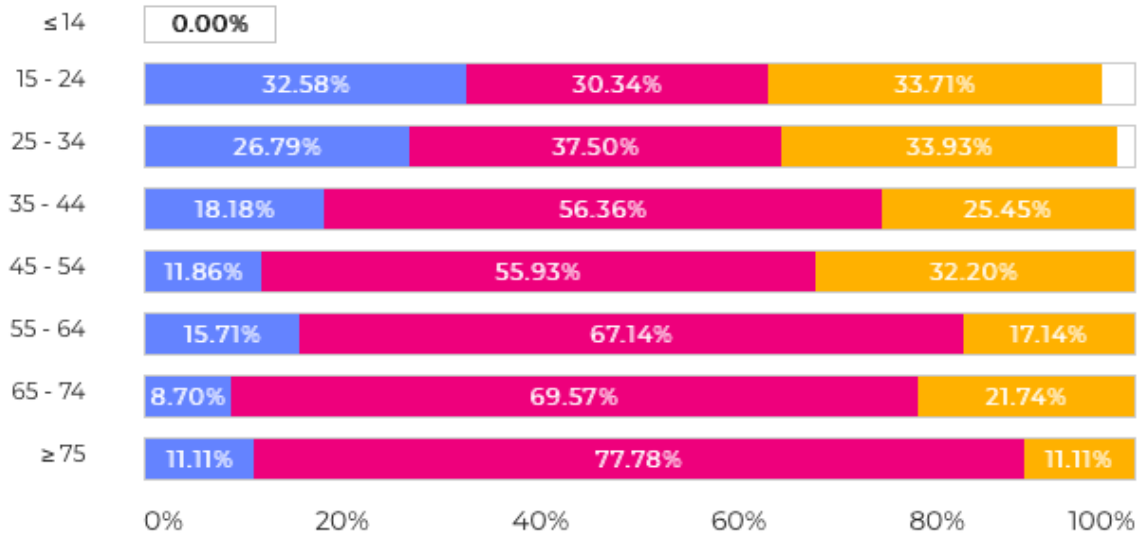
Insight 3: Those who trusted either NGOs or none of the 4 options to handle their personal data tend to agree with the fear more than those who trust the public service.



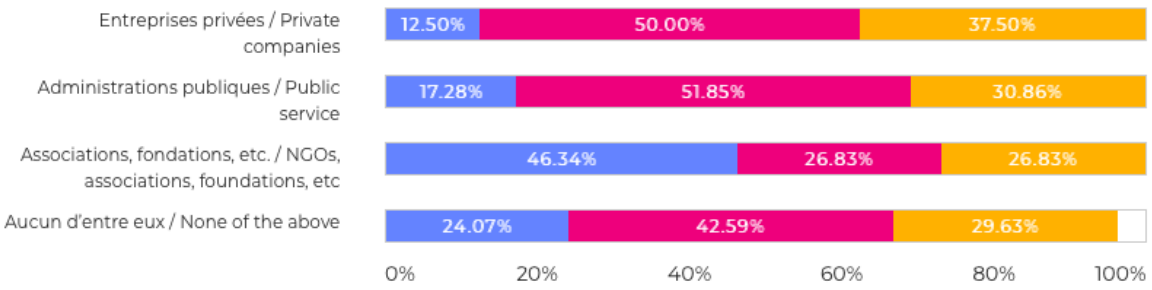
Statement 13:

"Partager des incidents sur les médias sociaux est plus efficace que de les signaler aux autorités. / Sharing incidents on social media is more effective than reporting it to the authorities."

Insight 1: There is a general trend where the older the participants, the greater the proportion of disagreement and the smaller the proportion of agreement and indecision.



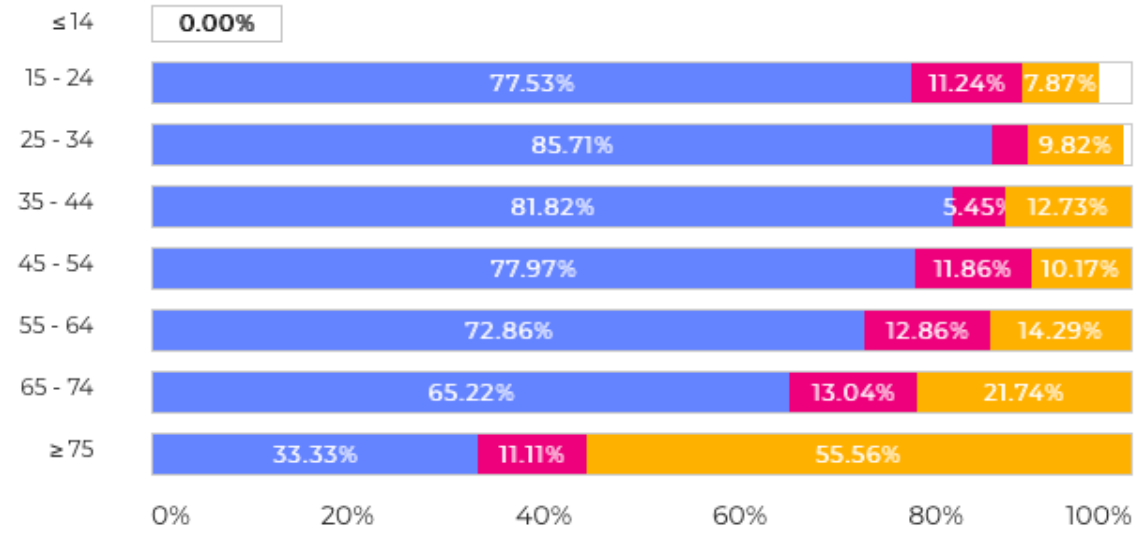
Insight 2: Those who trust NGOs with their personal data have about twice the likelihood to agree with the statement than those who trust the public service or none of the above. There could be one possible interpretation whereby those who trust NGOs see them as a check and balance to the authorities or a complementary force to the authorities for such incidents.



Statement 14:

"La dépendance aux technologies et la réduction de la durée d'attention ont créé un problème de santé publique. / Addiction to technologies and the reduction of attention spans has created a problem to public health."

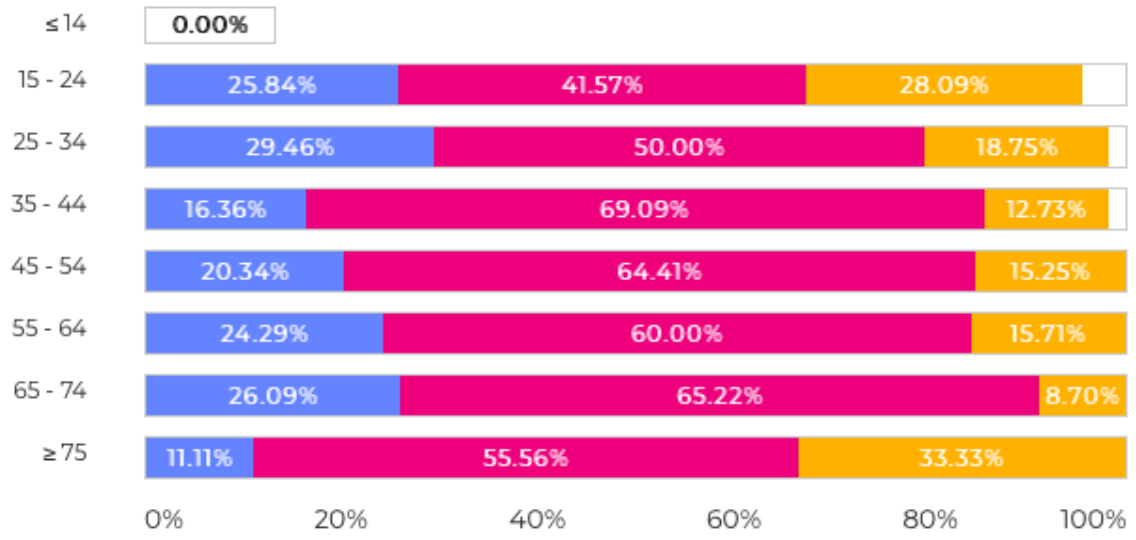
Insight 1: While there is overwhelming agreement across all age groups, the agreement is more intense as the age-group is younger.



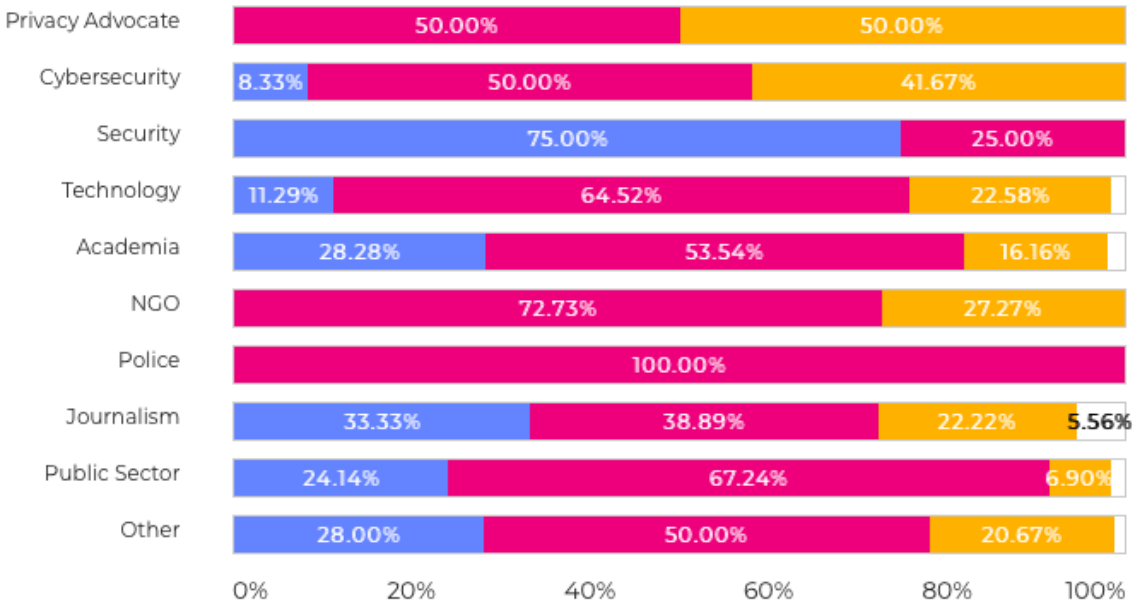
Statement 15:

"Le processus d'accès et de remplissage des formulaires administratifs numériques de la ville et du canton est difficile pour moi. / The process of accessing and filling up digital city and cantonal administrative forms is difficult for me."

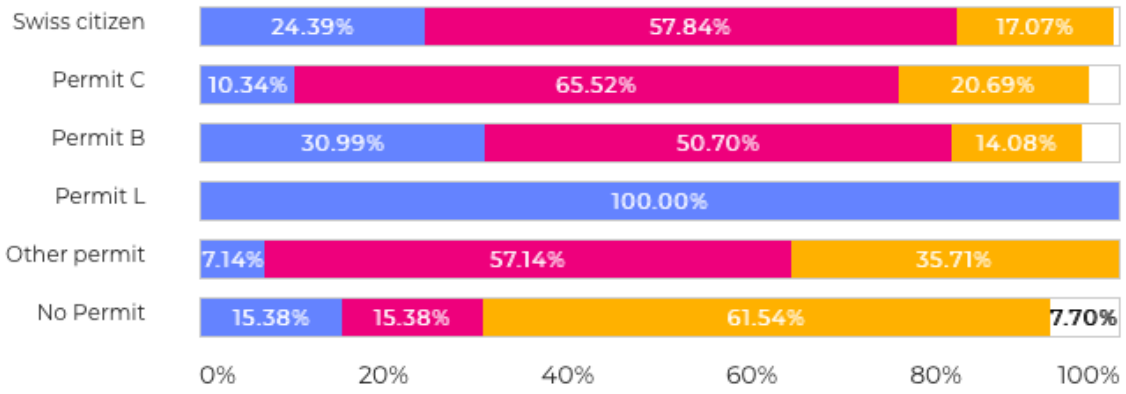
Insight 1: The trend line of increasing difficulty starts from the age 35-44 group onwards. Those of younger age groups face similar challenges as with the 65-74 age group with the exception of 15-24 year olds who have a significant proportion who are undecided.



Insight 2: Those working in the technology sector faced the least difficulty with online government forms.



Insight 3: Those with Permit C faced the least difficulty followed by the Swiss citizens and then Permit B holders. Permit C holders could have had more experience to fill up these forms.



Salient Comments from respondents:

Here are some of the more pertinent comments from the respondents that could give us more textured qualitative nuances and reasons for the responses by the respondents .

S/N	Statement	Theme	Salient Comments
1	Je crains pour ma sécurité physique dans les espaces publics (p. ex., les parcs et les rues) de Genève. / I fear for my physical security in the public spaces (e.g. parks and streets) of Geneva.	Physical Security	While a majority of the people feel safe, there are certain exceptions especially at night, in trains and with regards to a specific segment of society, which could be symptoms of seemingly deeper social and possibly economic issues that have not been addressed. *- Il faut toutefois faire preuve de bon sens pour limiter les risques ; Genève n'est pas une ville sûre en soi.* *- Les technologies de surveillance ne sont qu'un pansement et non la solution aux problèmes d'insécurité.*

			- drogue mendicite bandes des jeunes sans culture *- je ne sors pas beaucoup de mes trajets habituels quand je suis appelé à sortir la nuit. Je ne suis donc pas très représentatif de l'arpentage d'une ville.* *- I don't feel scared at all, except a little bit in the train station area.* *- Growing up in Geneva, I've never felt unsafe or in danger whatsoever. On the other hand, recently I feel that security issues are rising up in Geneva and its surrounding. Insecurity is still not at the level of other europeans countries but recent acts of senseless violence* *- Dépend de l'heure (plus c'est tard plus c'est stressant)*
2	La digitalisation croissante de ma vie sociale et urbaine est un problème majeur pour moi. / The increased digitalization of urban and social life is overwhelming for me.	Overwhelm from increased digitalisation	The complex layers of the comments suggest why this statement was the most divisive in the entire conversation as there are powerful private sector, democratic, historical and political forces at bay not forgetting the digital divide. *- Ce n'est pas la digitalisation en tant que telle: c'est l'aliénation à des puissances étrangères et des processus non-démocraties et obscurs qui pose problème.* *- La digitalisation peut être positive si elle est concrétisée correctement. Hélas aujourd'hui tous les efforts sont à double tranchant et amènent de gros problèmes de la sphère privée.* *- A ma connaissance, la sécurité dans notre espace publique n'est pas moins*

			bon qu'auparavant (je pense aux 50 dernières années). *- Je suis consciente de l'emprise de GAFAM sur nos vies, mais la numérisation de services de mon administration ne me pose pas de problème* *- J'en ai tout simplement marre de devoir consulter mon téléphone portable à tout bout de champ, d'attendre des codes de sécurité, de devoir me rappeler les logins et mots de passe que je n'ai pas pris soin de mettre dans une liste, d'être obligé de me racheter un tél... etc... etc* *- Formidable outil au potentiel infini, mais graves dérives assurées car inhérentes au néolibéralisme à tendance intrinsèquement totalitaire.*
3	Je crains la présence accrue de la surveillance numérique dans ma vie quotidienne. / I fear the increased presence of digital surveillance in my daily life.	Digital Surveillance's influence on daily life	The comments suggest a need to study surveillance from the private sector and public sector lens with an emphasis on the rights of individuals to their data and to seek recourse when their rights are violated. *- Où vont mes données* *- Notamment la mise en place de caméra et de système de reconnaissance faciale* *- Si on se fait agresser ou autre, c'est le parcours du combattant pour accéder aux vidéos* *- Je crains la surveillance des entreprises privées, pas celle de l'état*
4	Je crains d'être victime d'escroqueries, de vols d'identité, de phishing	Victim of digital crimes	The comments suggest that the elderly and less educated could be vulnerable to digital fraud and there could be a need to

	et de fraudes financières. / I fear being a victim of scams, identity thefts, phishing and backing/financial frauds.		raise awareness and educate people to keep their digital identities and data safe and secure. *- Et si il y a un bug? Je me retrouverai avec l'impossibilité d'accéder à mes propres données. Example plus d'accès à mes comptes bancaires etc.* *- Je crains pour les personnes âgées et moins éduquées, mais pas pour moi* *- C'est pour l'identité numérique cette question et pour l'argent numérique je suppose! Et vous n'en parlez pas quelle honte*
5	La plupart des gens ne signalent pas les crimes numériques (p. ex. le piratage ou le harcèlement en ligne). / Most people do not report digital crimes (e.g., being hacked, digital harassment).	Reporting of digital crimes	The overwhelming agreement and consensus suggests that the downstream justice and law enforcement response has not been sufficiently well developed to cope with digital crimes that are evolving at a much faster pace than the system can keep up with. However there are some individuals who believe the first line of defence lies with the individuals themselves. *- je me sens bien protégé par les outils informatiques que j'utilise (filtres spam etc... J'ai appris à couper court à des conversations ou relations épistolaires désagréables ou potentiellement dangereuses.* *- Les crimes numeriques ne sont pas suffisamment pris en charge par la justice quand ils sont signales*
6	Les autorités genevoises sont bien équipées et compétentes pour	Competence of Geneva	The strong level of disagreement and indecision shows that more needs to be done by the authorities to earn back the trust of the people's digital lives. There is

	protéger ma vie numérique. / The Geneva authorities are well equipped and competent to protect my digital life.	authorities	a strong call for national-level open-source initiatives to protect citizens' digital lives against private sector or criminal interests. *- Nos autorités ont des années de retard. Il est temp d'ouvrir des fondations open source (et pas des initiatives cantonales mais national voir transnational) pour offrir une alternative crédiables tant aux GAFAM qu'aux hackets de tout poil.* *- Je souhaite une instance étatique et démocratique qui s'empare de la protection de nos données envers les GAFAM.*
7	Je me sentirais plus en sécurité si la police et le gouvernement utilisaient davantage de technologies pour me protéger. / I would feel more secure if the police and the government used more technology to protect me.	Openness to police and government to use technologies for protection	There could be a need to address the perception-reality gap between what people think is happening to them and what is actually happening with regards to the topic of surveillance. More needs to be done to build public confidence in surveillance technologies. *- La surveillance de masse me ferait bien plus peur que les risques existants.*
8	Je crains que les données que le gouvernement genevois possède à mon sujet soient utilisées de manière inappropriée. / I fear that the data the Geneva government has about me is improperly used.	Mis-use of data by Government	The qualitative and quantitative response by respondents seem to suggest the 'double-edged sword' nature of technology, where it can be both a force for good and a force for bad. The fact that this is a highly divisive statement suggests the need for a "public-people-private" sector partnership to explore the arguments from both sides and the need to sensitise members of the public to the nuances embedded on both sides so that society

			can progress more delicately and artfully towards consensus on such matters. *- One the one hand, I feel that being up to date with modern security tools is crucial for the authorities and on the other hand it gives more power to them to spy and enter our privacy....*
9	Je crains que les décisions concernant ma vie quotidienne (p.ex. travail, santé, logement) soient de plus en plus prises par des algorithmes. / I fear that decisions about my daily life (e.g., work, health, housing) are increasingly made by algorithms.	Algorithmic influence on daily life	More spaces for dialogue and greater understanding on the impact of algorithms on people's daily decisions could be convened to mitigate the risks of algorithms. *- Ce que je crains, ce sont les décisions prises par des algorithmes dont la sécurité n'a pas été éprouvée. S'ils sont bien conçu, ils ont beaucoup de bonnes choses à apporter* *- A Genève ce n'est toujours pas le cas, mais je pense que ça va arriver* *- Je pense que c'est le cas, mais cela ne me dérange pas forcément*
10	Je crains que les grandes entreprises technologiques (ex. Facebook, Google) utilisent mes données sans que je m'en rende compte. / I fear that big tech companies (e.g. Facebook, Google) are using my data for purposes I am unaware of.	Awareness of use of data by Big Tech	The comments seem to suggest that it is in big tech companies' interest to maintain a degree of information asymmetry between what big tech knows and what people know. This requires independent and expert panels who are able to have the same level of expertise to understand and keep up with the intricacies and dynamics of big tech. *- Je crains de donner mon accord involontairement à l'enregistrement de données en clickant très vite sur des accords me permettant de lire un article ou d'autres accords pour garder mes*

			coordonnées lors des achats en ligne depuis Facebook. *- Je ne le crains pas, je le sais...* *- Ce n'est plus un crainte, c'est un fait* *- l'utilisation de mes données ne m'inquiète pas. je fais en sorte de ne pas trop me dévoiler sur internet afin de me sentir confortable même si je suis conscient que je ne maîtrise pas grand-chose et ne comprends pas tout.*
11	Je crains que les données que les entreprises privées (ex. Facebook, Google) détiennent à mon sujet soient utilisées de manière inappropriée. / I fear that the data private companies have about me is improperly used.	Misuse of data by Big Tech	Based on the comments given by the participants, we can sense resignation and 'learned helplessness' by the respondents. This seems to suggest the power has tilted too favourably in the hands of private companies and society has to have a countervailing force to keep them in check. The qualitative and quantitative data gives us the endorsement, 'green light', impetus or credibility to galvanise society to address this problem through greater public and people sector intervention and debate. *- Il est déjà trop tard* *- Je ne le crains pas, ça aussi je le sais...* *- C'est deja la cas*
12	Les médias sociaux sont une source crédible d'informations et de nouvelles pour me tenir au courant des menaces de sécurité à Genève. / Social media	Credibility of social media	The source of disagreement from the respondents point to bias, echo chambers, credible sources and the ability of the reader to discern and corroborate.

	is a reliable source of information and news to keep me aware of security threats in Geneva.		*- Les médias sociaux comportent d'énormes biais, représentent un terreau fertile pour la manipulation de masse (ex : Cambridge Analytica) et représentent une chambre d'échos qui conforte les participants dans leurs croyances.* *- Si les sources sont bonnes et que les algorithmes les promeuvent* *- Dans les médias sociaux, la fiabilité dépend des émetteurs: enquêtes soignées des grands médias par exemple ou journalistes confirmés qui respectent la règle des 3 sources* *- Toutefois, il faut pouvoir distinguer, corroborer et être critique par rapport à la source et le contenu de l'information.*
13	Partager des incidents sur les médias sociaux est plus efficace que de les signaler aux autorités. / Sharing incidents on social media is more effective than reporting it to the authorities.	Sharing incidents on social media	Despite the fact that the majority disagree, the indecision and disagreement suggest that the complications brought about by the bubble of social media has complicated the equation significantly, introducing multiple possible responses depending on the nature of the situation, response and the authorities. This is an area of nascent development that requires a more concerted people-public-private sector deliberation that could be stress-tested with a series of scenario-planning exercises. *- J'aurai tendance à faire les deux* *- Cela dépend du type d'incident, de la réponse attendue et du travail effectué par les autorités.*

			- Cela permet toutefois de sensibiliser chacun sur les risques, mais pas de dire comment s'en protéger. Et sans implication des autorités, pas d'arrestation
14	La dépendance aux technologies et la réduction de la durée d'attention ont créé un problème de santé publique. / Addiction to technologies and the reduction of attention spans has created a problem to public health.	Addiction and attention span on public health	A very high majority of 79% of respondents who agree with the statement and the qualitative comments below seem to suggest this is a very important problem that is not treated urgently, but it is a 'ticking time bomb' ready to implode in the near future if we do not take pre-emptive or proactive steps to addressing the issue. The comments seem to suggest that the problem is out of control and very complex, thus requiring multiple stakeholders to come together to co-operate. *- In my opinion, not to public health, but to the ability of taking informed decisions for the general population: misinformation, mistrust, misplaced role models, etc. Nothing that was not happening before, technology has simply made it explode.* *- Un problème MAJEUR. Nous sommes dans une analogie à l'épidémie d'opium il fut un temps en Chine.* *- https://rune-geneve.ch/* *- Le problème risque de devenir grand à l'avenir mais pour l'instant, d'autres problèmes de santé publique me paraissent plus importants*

15	Le processus d'accès et de remplissage des formulaires administratifs numériques de la ville et du canton est difficile pour moi. / The process of accessing and filling up digital city and cantonal administrative forms is difficult for me.	Digital admin forms	The fact that there is a majority 56% that disagrees with the statement does not mean that we should ignore the minority 25% who have made 5 very important qualitative remarks below that need to be taken seriously and urgently by the authorities administering these forms. This shows the importance of diving deeper into the sentiments and feelings of the minorities even though there is a majority public opinion that thinks differently. A policy development framework based on the philosophy of 'centering the margins' ought to be adopted to bridge the gap between the digital literates and non-literates. *- Le fait que le remplissage des formulaires n'est pas difficile pour moi ne signifie pas que d'autres ont sont souvent démunis vis-à-vis de la cyberadministration. Il faut que l'option "analogique et humaine" reste une alternative.* *- Le gros problème avec les formulaires numériques est que l'on est contraint aux champs et formats spécifiés. Le formulaire papier permet de rajouter des notes et le remplir librement.* *- Pour moi je dirais que non. Comme travailleuse sociale qui accompagne des personnes en situation de précarité ou sans domicile, je constate que l'accès et le remplissage est difficile pour une grande majorité des personnes que je côtoie* *- Mais c'est difficile pour toute une catégorie de la population, en particulier personnes âgées et personnes allophones*

			- I would say it's more than difficult, it is oppression
16	Je suis d'accord que mes données personnelles récoltées par les administrations publiques soient hébergées sur des serveurs à l'étranger. / I agree to have personal data collected by the government to be stored in servers outside Switzerland.	Storage of personal data in foreign servers	While a majority of respondents disagree, some creative workarounds or new ideas revolve around decentralisation on the blockchain and having the data on servers where there are existing agreements and ties. *- Une piste intéressante semble être la décentralisation des données et la mise à profit de la blockchain pour voir peut-être émerger un jour une économie plus saine de la data.* *- Tout dépend où se trouvent les serveurs : en Europe, cela peut être acceptable car des accords existent*
17	J'ai déjà envisagé ce scénario: des services numériques, utilisés quotidiennement, inaccessibles pendant une durée indéterminé. / I have already imagined a scenario where digital services that I use daily are unavailable for a period of time.	Interruptions in digital services	One comment suggested that the statement could be improved in its formulation.

Open Ended Comments -
Below are some open-ended comments from participants that may or may not be linked to the 17 statements

Physical Security

1. *Intro mentions burglary, but there is no question about it. My perception of the safety of apartments in Geneva is weak compared to my origin*

country (e.g quality of doors). Possibly related to the fact that are owned or managed by real state agencies not willing to spend enough.

Education, Raising Awareness and Consciousness

2. *Sensibilisation des enfants et jeunes*

3. *Pensez-vous que les jeunes utilisateurs de smartsphone sont correctement accompagnés par leur entourage dans l'utilisation de ceux-ci?*

4. *Sentez-vous une différence de sensibilité entre les générations au sujet de toutes ces questions de "privacy" ? Quand (en quelle année) le monde du formulaire physique s'arrêtera-t-il (tout en ligne) ?*

Lack of Public Discourse

5. *Le manque d'informations et de débats, sur ces questions dans l'espace public.*

Perception versus Reality

6. *Les questions sont assez biaisées. En sociologie, il n'y a pas toujours de corrélation entre sentiment de sécurité et situation sécuritaire réelle. De même, sur internet, on ne sait que ce qui nous traque. Donc on peut se sentir en sécurité alors qu'on ne l'est pas.*

Pace of digitalization - too fast and too far

7. *La question de la surveillance numérique est indissociable à l'expansion du secteur, aussi pour des questions environnementales. Pensez-vous que la numérisation de la société va trop loin et trop vite ?*

Degree of social media usage as MCQ for slide-and-dice analysis

8. *Poser des questions sur le degré d'utilisation des reseaux sociaux aiderait à mettre en perspective les autres reponses*

Penetration testing, risk mitigation, recovery and resumption of service by canton

9. *Le canton est-il suffisamment bien préparé à faire face à une cyber attaque, à assurer la continuité de service des services essentiels*

(énergie, gestion et traitement des eaux, système de soin,...) en cas de cyber attaque.

AI Ethics

10. *Je conseillerai la série de vidéo sur l'éthique de intelligence artificiel de Science4All sur YouTube. Ici: https://youtube.com/playlist?list=PLtzmb84AoqRRFcoGQ5p7kqEVQ7deXfYuH Ainsi que le livre "Le fabuleux chantier " de Lê Nguyên Hoang, sur la sécurité des algorithmes.*

Single point of failure by a bug

11. *La crainte d'un grand bug qui efface toutes les données et enlève toute l'accessibilité aux cations courantes dont nous avons pris l'habitude: paiements, gestion à distance, pannes (ascenseurs, etc.)*

Checks and balances, transparency and citizen verifications

12. *Pouvons-nous consulter les données accumulées par les autorités genevoises?*

Responding to identity thefts

13. *Est-ce que vous vous sentez bien protégé contre les conséquences de l'usurpation de votre identité (par exemple pour effectuer des achats en ligne, des publications en votre nom ou effectuer des actes illicites) et savez bien comment réagir ?*

Post quantum cryptography of Geneva's data security

14. *Qui sont les acteurs privés de la sécurité des donnés à Genève actuellement sous mandat avec la ville / l'état ? I à t'il des projets d'identité numérique cryptés en post quantum? Si non pourquoi?*

Guarding against deep fakes and reasonableness of precautionary measures

15. *Comment se prémunir des deepfakes? Quelle politique personnelle de gestion des données adopter, lorsque l'on sait que même les grands du numérique se font hacker? J'ai peur d'être un jour victime de ramsomware et je ne suis pas certain d'avoir pris toutes les précautions utiles.*

Personal list of measures to protect private data

16. *Quelles mesures avez-vous pris pour protéger vos donnés privées ? VPN Browser spécifique (eg duck duck) Utilisation restreinte des réseaux sociaux Gestionnaire de mots de passe Autres Aucunes*

Recommendations and Conclusion

Using the 'Axis of Fear', 'Axis of Agreement', Decision Matrix and crowdsourced comments as inspiration, we have put together a list of 9 'High Level' recommendations from recommendation A to recommendation I that can be broken down into 19 'Lower level, detailed or granular' recommendations of which 17 are tied to the 17 seed statements and the remaining 2 are tied to the open-ended comments in the qualitative section of the poll results.

THE WHO?	**Alliance or Sector**	**Public Sector (Police and Digital Government Services)**	**Public Sector (Physical and Mental Health and Wellbeing)**	**TriSector (People-Public-Private Sectors) Alliance Taskforce for Action**
THE WHAT?, HOW? and WHEN?	**Priority1 (Immediate Implementation - Urgent and Important)**	A. Rebuild Digital Trust in Government	B. Heal and Mitigate the Negative Impact to Public Health and Safety	C. Exert a Strong Check and Balance on Big Tech Companies
	Priority 2 (Immediate to Delayed Implementation - Quite Important but not Urgent)	D. Strengthen Societal Awareness and Response to Digital Crimes and Frauds E. Nurture Safe and Accessible Channels (or Portals/Hotlines) for Digital Crimes Reporting F. Prepare Society to Respond to Interruptions in Digital Services	-	G. Harness the Power of Social Media
	Priority 3 (Delayed Implementation - Not Urgent or Not Important)	H. Make Digital Form Filling More Accessible I. Address Lingering Physical Insecurity issues	-	-

To help us visualise these recommendations, we have categorised these recommendations into a 3X3 matrix where the:

a. Horizontal axis refers to the different actors in society who should lead and take charge of and be accountable for these recommendations and the
b. Vertical axis refers to the priority level that the recommendations are classified under so that appropriate resources can be allocated to the right set of recommendations in different time-frames.

The vertical axis does not only include the dimensions of “what” and “when” but also “how” so that readers of this report can imagine pathways of possibilities that are actionable. This can give society a sense of progress and the confidence that something is being done to address the issues raised in the discussion.

THE WHO?	Alliance or Sector	Public Sector (Police and Digital Government Services)	Public Sector (Physical and Mental Health and Wellbeing)	TriSector (People-Public-Private Sectors) Alliance Taskforce for Action
THE WHAT?, HOW? and WHEN?	**Priority1 (Immediate Implementation - Urgent and Important)**	A. Rebuild Digital Trust in Government by - Ensuring proper use of personal data of citizens and residents (s8) - Allaying fears by citizens on increased presence of digital surveillance in their daily lives (s3) - Addressing citizen's perception of safety and security in the use of technologies for their protection (s7) - Improving Competence and Equipment of authorities to protect digital lives of citizens (s6) - Stopping storage of personal data in foreign servers (s16) How? - Deliberative democracy frameworks such as Citizen Panels, Citizen Review Committees and Citizen Town Hall Meetings[4] - Tools such as Experimental Sandboxes in physical and virtual spaces - Facilitation methodologies such as Theory U to allow new fears and issues to emerge and existing fears to be allayed - Invest in human-centred design capabilities and equipment - Demo and Exhibition Day during Swiss National Day	B. Heal and Mitigate the Negative Impact to Public Health and Safety by - Addiction to technologies and reduction of attention spans (s14) - Fears by citizens from algorithms taking over decisions about daily life (s9) - Overwhelm felt by citizens from the increased digitalization of urban and social life (s2) How? - Expert panels and review committees on the impact of algorithms - Community-based Participatory Research to unpack and shed light on the private sector, democratic, historical and political forces that have led to a sense of overwhelm by the public.	C. Exert a Strong Check and Balance on Big Tech Companies in - Transparent and Proper use of personal data (s10, s11) - Policy development architecture and framework whereby policy clockspeed matches the unrelentingly fast clock speed of technological developments (open-ended) How? - Participatory Democracy frameworks such as vTaiwan's 15 step process[5], Citizen Panels and Citizen Review Committees - Led by citizen-backed and expert Non-Governmental Organisations such as Center for Humane Technology - Independent 3rd party audits of transparency and proper use of personal data distributed through reports or a online web observatory

[4] For example, https://participedia.net/# is a global network and crowdsourcing platform for researchers, educators, practitioners, policymakers, activists, and anyone interested in public participation and democratic innovations. There are 2222 case studies, 355 methods for us to draw inspiration from.

[5] For example, at least 26 national issues have been discussed via vTaiwan and more than 80% have impacted policy outcomes and led to decisive government action. The results of the vTaiwan process have been at the core of 11 laws and regulations. A few articles on vTaiwan, participative democracy and wiki-surveys are here: https://congress.crowd.law/files/vtaiwan-case-study.pdf and https://www.centreforpublicimpact.org/case-study/building-consensus-compromise-uber-taiwan/

	Priority 2 (Immediate to Delayed Implementation - Quite Important but not Urgent)	D. Strengthen Societal Awareness and Response to Digital Crimes and Frauds by - Having a digital crimes and fraud awareness month in schools, community spaces, workplaces and public spaces (s4) - Creating mechanisms in place to help citizens and residents prevent, report and address digital crimes in a timely manner with the police and judicial system. (s4) - Having an up-to-date repository of the list of practical measures that citizens can implement to keep abreast of the evolving nature of security threats e.g. post quantum-cryptography, prevention against deep-fakes, ransomware and many more invisible threats (open-ended) E. Nurture Safe and Accessible Channels (or Portals/Hotlines) for - Digital Crime Reporting and Remediation (s5) F. Prepare Society to Respond to Interruptions in Digital Services by - Developing Scenarios, Stress Testing and Response Plans to Interruptions in Digital Services (s17) How? - Participatory Action Research (PAR) to understand barriers to reporting and human-centred design to design UI/UX-friendly channels/portals or hotlines - Coordination between Police, Judiciary and Citizens to respond quickly to the evolving nature of digital threats	-	G. Harness the Power of Social Media as - A reliable source of information and awareness of security threats in Geneva (s12) - An effective channel for reporting and sharing about incidents that complements formal reporting channels to the authorities (s13) How? - Open Space Technology (OST) tools such as Unconferences or World Cafes to bring in ideas and strategies from diverse segments of society in a spirit of asynchronous co-creation over the course of weeks in a digital and physical space that is accessible to diverse members of society.

	Priority 3 (Delayed Implementation - Not Urgent or Not Important)	H. Make Digital Form Filling More Accessible - For a minority of digitally illiterate or marginalised segments of society (s15) I. Address Lingering Physical Insecurity issues in - Public and Private Spaces in Geneva by addressing the socio-economic roots of the problems(s1) How? - Participatory Action Research (PAR) to understand and address underlying socio-economic root causes to the problem of physical security in Geneva. - A policy development framework based on the philosophy of 'centering the margins' ought to be adopted to bridge the gap between those with digital literacy and those without. - Improvements in User Interface (UI) or User Experience (UX) design of the forms - Having virtual assistants or physical assistants in dedicated clinics for digital form filling - Social Science research methodologies such as Ethnography and Design Thinking - Broken Windows Theory to help nip physical security issues in the bud as they manifest and fester	-	-