
Hello bank!
Trendwolves
ONLINE PRIVACY:
A FOLLOW-UP SURVEY

A research report by **Trendwolves** for

Hello bank!

October-November 2017

info@trendwolves.com

1. INTRODUCTION

This report discusses the key-findings of a quantitative survey on how young people in Belgium feel, think and act with regard to **online privacy**. This is a **follow-up study on a report we published in January, 2016**. Almost two years after this survey, our main research question today is whether we can observe **meaningful changes over time** in how people think about online privacy.

In the previous report, we outlined four "**privacy profiles**", based on two key characteristics: privacy concerns (how concerned people are about their online privacy) and privacy behavior (how much action people undertake in order to safeguard their online privacy):

1) **Apathetics** combine low privacy concerns with low privacy enhancing behavior. They don't really care about (their) online privacy.
2) **The Mainstream profile** (the biggest and most "average" group, around 40%) combine less-than-average concerns with higher-than-average actions. We speculated that this group is less concerned *because* of the actions they undertake to safeguard their privacy.
3) **The Privacy Priests** are very concerned about their online privacy and take actions, but they also feel that they can "never to enough" to protect their privacy.
4) **The Fatalists** are those who are very concerned but also feel that "they can't do a whole lot about it". In sum, this is the group that seems to have "given up" on their online privacy and as a result don't take a lot of actions to protect their privacy online.

Along with constructing a typology, we focused on some other important privacy dimensions, such as **privacy negotiation** (how willing people are to exchange their personal information for certain benefits), **privacy awareness** (how aware people are of their online privacy) and **privacy knowledge** (how educated are people about online privacy?).

This study will focus on evolutions in these concepts over an (almost) two-year period and is in this sense unique. Although online privacy mostly became a very hot topic following the high profile **Edward Snowden & NSA case in 2013**, online privacy became much more than a ripple in the pond. In the last years, **online privacy has become more than an individual issue - it has conquered its place in the highest policy regions as well**. In 2015, Trendwolves spotted and has written about a trend amongst youngsters they named "Crypto Culture". This trend was all about "avant-garde youngsters actively exploring the possibilities of the "dark web" and data encryption to protect their online identities.". In short: privacy

What we have written in 2015 still applies today and if it has changed in any direction, it's most likely in the direction of an intensification: "In the past years, **commercial businesses have discovered the internet as a new playground for advertising and marketing**. Along with the

mind-boggling expansion of social network sites such as Facebook, Twitter and LinkedIn, **methods of targeted marketing and advertising have been rapidly developed**. Rather than paying for large scale mass-media targeting, businesses spend big on methods that allow targeting their audiences based on their cultural preferences, social characteristics, locations, or demographic profile. Data is marketable. It's big business… And this fact forces people to take think about their role in this story."

Governments and businesses seem to have gotten convinced that **data is indeed a "new gold" that can be exploited**. In this report, we try not to take a stand in the debate but rather we seek to understand how different people think differently about online privacy. We're still looking for shades of grey rather than more activist black-and-white perspectives on privacy (from whatever perspective!).

We will paint our picture on online privacy again and look at how the hues and colors of that picture changed, if they changed at all. Let's dig into it.

2. RESEARCH POPULATION AND -QUESTIONS

In this survey, we are interested in **how young people deal, in the broadest sense, with (their) online privacy**. We therefore took a sample of 750 men and women in the Belgian population. Ages of the respondents range between 18 and 40. We noted in our earlier report that, although a lot of research has been invested in how youngsters/ adolescents deal with online privacy, much less has been written about the specific age category of people in their thirties. The age-group demarcations in this study are very interesting in the sense that we have three distinct groups when it comes to *online* privacy. The **youngest group are digital natives**: the internet has been around since they were born. They know no "other" world. The group of **people in their thirties has seen the rise of the internet at a relatively young age**, so one would expect them to be flexible adaptors to these new technologies. However, certainly those **deep in their thirties, are old enough to have been brought up with a more "old school" scheme of privacy**, where privacy was seen more as a fixed and "automatic" rather than a flexible and "active" concept.

Our main research questions are the same as our study in 2015/2016. We're still interested in the most important privacy concepts and how they are spread across the population in Belgium. However, one important extra focus will be on the ***shifts* in how our research questions have been answered by the respondents**. We're interested to see if, and in which ways, we can see changes in our fundamental privacy concepts.

The key concepts and questions of our study are:

1) **Privacy knowledge**: what do young people know about (how to protect their) online privacy?
2) **Privacy concerns**: to what extent are they concerned about their online privacy?
3) **Privacy negotiation**: to what extent are young Belgians willing to exchange personal information for benefits of all kinds?
4) How do these **concepts relate** to each other? What are the most important group differences?
5) Can we still observe the **privacy typology** of Mainstream, Privacy Priests, Fatalists and Apathetics? How has this shifted over the past 2 years?

It has to be noted of course that the people in this study are mostly *different* people than in the first empirical survey, which makes room for a certain margin of error in our analyses. This statistical fact, rather than a "real evolution" in the population, will undoubtedly account for small changes in numbers. We will focus on the bigger picture. We shouldn't mistake "big shifts" for "meaningful findings", however. **It certainly will be meaningful when we *do not* find big trends, as this will suggest that feelings and attitudes about privacy have "stagnated" or "balanced out"**. The implications of this are just as important as the implications of bigger shifts.

Before we start with our own data and analyses, let us first look at the very concise literature review about privacy.

3. A VERY FAST TRIP THROUGH PRIVACY LITERATURE

In this section, we mostly build upon our earlier literature review. In the past 2 years, no *game-changing* articles have been published that *fundamentally* alter the way we look at online privacy. However, **new ways of conceptualizing privacy in online contexts emerge and are constantly being developed further**. One such important new concept is "**networked privacy**", first sketched out in a widely cited paper of Marwick[1]. By conceptualizing privacy **not as an *individual issue* but rather as a socially negotiated action**, they create room for thinking about privacy as something that happens in *contexts* that have *boundaries* that can break. The concept of "**privacy turbulence**" fits in here well. It refers to situations in which boundaries (e.g. "public <-> private") break down and disclosure of personal information flows into the public sphere. Think about a youngster posting a photo on Facebook that unintentionally "goes viral". A relatively new theory linking these concepts is called "**communication privacy management**", which places central importance on these boundaries and decision processes of people regarding their online privacy.

It seems clear, in any case, that new theories and research increasingly adapt to the new fluid online contexts we are all surfing in. **Our understanding of online privacy deepens as theorists gradually steer away from older and increasingly redundant notions of privacy from before the Digital Age**. In the following sections, we review our key concepts of privacy.

3.1. PRIVACY CONCERNS

Privacy concerns refer to how alarmed people are about their online privacy. People that worry a lot about their online privacy, score high on privacy concerns.

Goldfarb & Tucker[2] looked into changes in privacy concerns over time between 2001-2008. They observed two important things when looking at how consumers deal with online privacy. First, "refusals to reveal information have risen over time" and secondly, they observed a large gap between how younger and older people deal with online privacy. Youngsters are much more likely to reveal personal information online, although they seem to have become "somewhat more private over time". They explain this by noting that, even though consumers were always privacy-protective in "typical privacy-sensitive" contexts such as health- and finance-products, **today more topics are seen as potentially personal.**
This finding points to something that is really important when thinking about privacy: **it's a constantly changing concept**. Because of this, there seems to be no agreement on what the concept actually stands

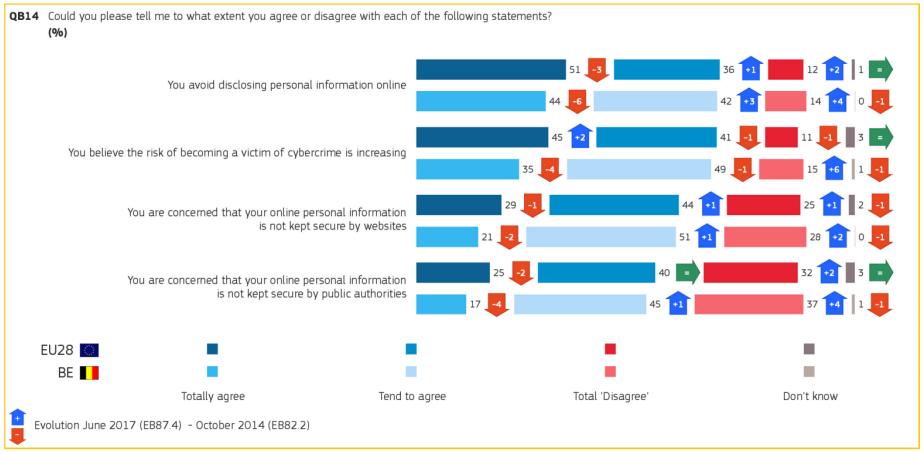
[1] Marwick, A.E. & Boyd, D. (2014): "Networked privacy: How teenagers negotiate context in social media" in New Media & Society 16(7): 1051-1067

[2] Goldfarb, A. & Tucker, C. (2012): "Shifts in Privacy Concerns" in American Economic Review: Papers & Proceedings, 102(3): 349–353

for. Indeed, we wrote in our previous research that "what seemed like outrageous intrusions of privacy yesterday, seem very self-evident and unproblematic tomorrow". For instance, when the Facebook Timeline got introduced back in 2006 (in which people could see real-time updates from friends in their social circle), some observers passionately outcried that this was a rude intrusion of privacy. Today, however, this Timeline is an essential and desirable feature of Facebook. New technologies and innovation always seem to trigger "privacy panic" in the beginning.

But people are right to be skeptical about their online privacy. The **OECD[3] identified privacy as the 3rd highest-priority policy area in digital economy** (after broadband availability and security). Indeed, "consumers are (…) increasingly paying attention to privacy in the digital environment. (…) 64% of respondents are more concerned about privacy than they were a year earlier *(in 2014, that is)*".

We noted in our earlier report that privacy concerns were alarmingly high in 2009 (based on Eurobarometer data). **The figure on the right shows very recent numbers regarding privacy concerns of a Eurobarometer survey in 2017 in Belgium[4]**.



We can observe that Belgians seem, on average, a little less concerned than the average European about internet privacy. However, 86% of the Belgians claim to avoid disclosing personal information online and 84% believe that the risk of becoming a victim of cybercrime is increasing although, it should be noted, that only 3% of the Belgians in fact *experienced* an online abuse of personal information[5]. On the other hand, according to the 2017 Eurobarometer, 36% of the Belgians claim to have received fraudulent emails or phone calls asking for your personal details (including access to your computer, logins, banking or payment information) and almost 1 in 5 claims to have had their social network or email account hacked.

[3] OECD Digital Economy Papers (2016): "Managing Digital Security and Privacy Risk: 2016 Ministerial Meeting on the Digital Economy"

[4] Special Eurobarometer 464a (2017): "Europeans' Attitudes Towards Cyber Security"

[5] See statistics on http://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database

3.2. PRIVACY KNOWLEDGE

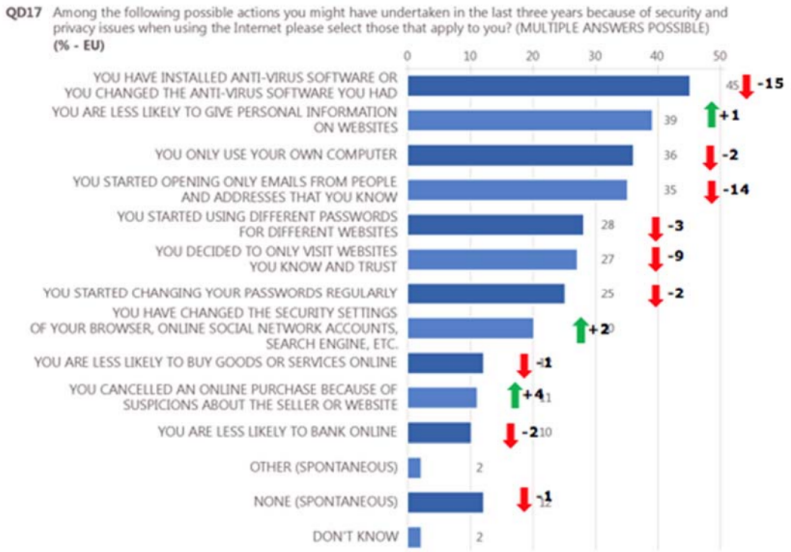
Privacy knowledge is knowledge about the "privacy-system" and how to protect online privacy. It contains **knowledge** about how apps/ services/websites collect and use personal data as well as the **skills** for privacy-enhancing behavior like erasing cookies, manually adjusting privacy settings and so on.

Privacy attitudes refer to how people think (cognitive element) and feel (affective element) about privacy. If refers to whether people think their privacy is something valuable or not. A consistent finding in privacy literature is that youngsters overestimate their knowledge about online privacy[6]. They have little knowledge about how their data is actually a commercial resource. The fact that online privacy disclaimers are not easily readable, often hidden or difficult to find, and the fact that the "data-as-a-business" system is well hidden from consumers, are crucial to this. **Research institutions in Belgium, along with youthwork organisations have stressed the importance of campaigns to increase not online privacy awareness but also privacy skills amongst youngsters in Belgium.**

3.3. PRIVACY BEHAVIOR

Privacy behavior can be seen as a **coping strategy in response to privacy concerns.** It means: changing your online behavior to actively protect your personal information and includes all the actions oriented towards this goal. Often cited examples in the literature are: providing false or incomplete information when filling in an online registration, installing specialized software (adblockers, anti-trackers), complaining when people are being sent unwanted email, using different passwords, etc.

Some research has pointed out that there are actually weak links between privacy awareness, concerns and behavior. People tend to have general ideas and feelings about privacy, but when faced with very concrete situations in which they have to provide personal data for perceived benefits (e.g. getting an account), they easily deviate



Base: Respondents who are Internet users (N=22,472. Results taken from the Special Eurobarometer 460 'Attitudes towards the impact of digitisation and automation on daily life.

[6] EMSOC report (2014): http://emsoc.be/wp-content/uploads/2014/08/D3.3.2_SMIT.pdf

from their grand ideas and concerns (see the important concept of the "privacy paradox")… Privacy is always a trade-off between concerns and actions.

Privacy behavior is the second axis on which we will build our privacy typology, resulting in 4 quadrants with low/high concerns and low/high privacy actions. The image above shows the results of the Eurobarometer in 2017 about privacy actions people in Europe take. Anti-virus software is the primary action people take, along with not giving away personal information on websites. However, these numbers don't even add up to half of the respondents, suggesting that, **eventhough people are very concerned, they do not take appropriate actions to protect their privacy.**

3.4. PRIVACY CONCERNS

Privacy negotiation refers to the **willingness to exchange certain personal information for benefits provided by companies**. Here aswell, we would expect the full continuum of opinions from those absolutely not willing to trade their privacy for benefits to those who are very willing to do so.

Privacy negotiation is an important concept as it hints that **privacy is an *active* rather than a *passive* concept**. Implicit in a "negotiation" is a context in which at least two parties negotiate. In a world where companies increasingly discover the power of customer data, we expect that privacy negotiation and the skills for this will only increase in importance.

A much mentioned side-concept of privacy negotiation is the privacy paradox, which refers to contexts in which privacy is at stake, sometimes without people even knowing. For instance, we would expect youngsters to be very wary of companies using their personal information to their own benefit. However, a recent study found that adolescents seem to react favorably to highly personalized ads, based on their personal information/interests[7]. The authors who found this explain this with the **privacy paradox**: **"Although consumers declare to be concerned about their (online) privacy, their concern contrasts with disclosure behavior in concrete situations."**

A consistent finding is that even though people value their privacy, when prices come in, people often put aside their concerns for personal benefits[8].

[7] Walrave, M.; Poels, K.; Antheunis, M.L.; Van den Broeck, E.; van Noort, G.: Like or dislike? Adolescents' Responeses to Personalized Social Network Site Advertising in: Journal of Marketing Communications

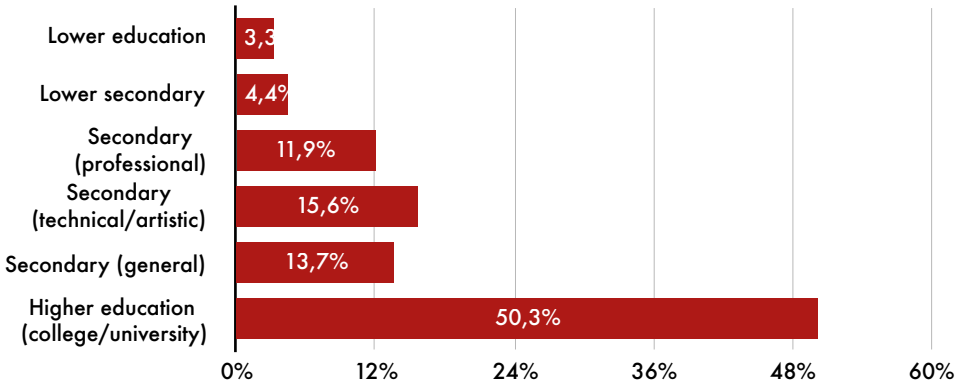
[8] Jentzsch et al. (2012): "Study on Monetising Privacy. An Economic Model for Pricing Personal Information"

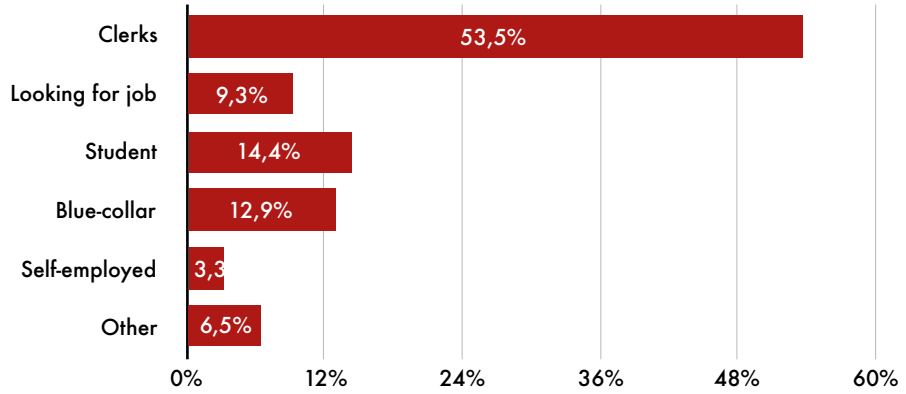
4. WHO ARE WE LOOKING AT?

This survey generated 750 completely filled in questionnaires, exactly balanced between **Flanders (50%) and Wallonia (50%)** and **men (49%) and women (51%)**. Ages range between 18 and 40 years old and educational level goes from primary school to university. Most respondents are highly educated.

In comparison to the 2015 survey, we have a slightly (but statistically significant) older group of respondents. The average age in the 2017 survey is **31 years old** compared to 29 in 2015. The only other statistically significant difference between 2015 and today can be found in professional status: there seem to be less unemployed respondents today (9,3% versus almost 20%) and the group of clerks is bigger than in the 2015 sample.

Along with the standard socio-demographic variables outlined above, we were interested to paint a general picture on general online behavior and to see whether we could see changes in internet usage between 2015 and 2017. Our results suggest that this is not the case. We still have **50% of the respondents claiming to be online for more than an hour per day**. We couldn't observe a statistically significant change in social media activity. A little less than a quarter of the respondents are active on social media in the sense that they regularly post on social media.

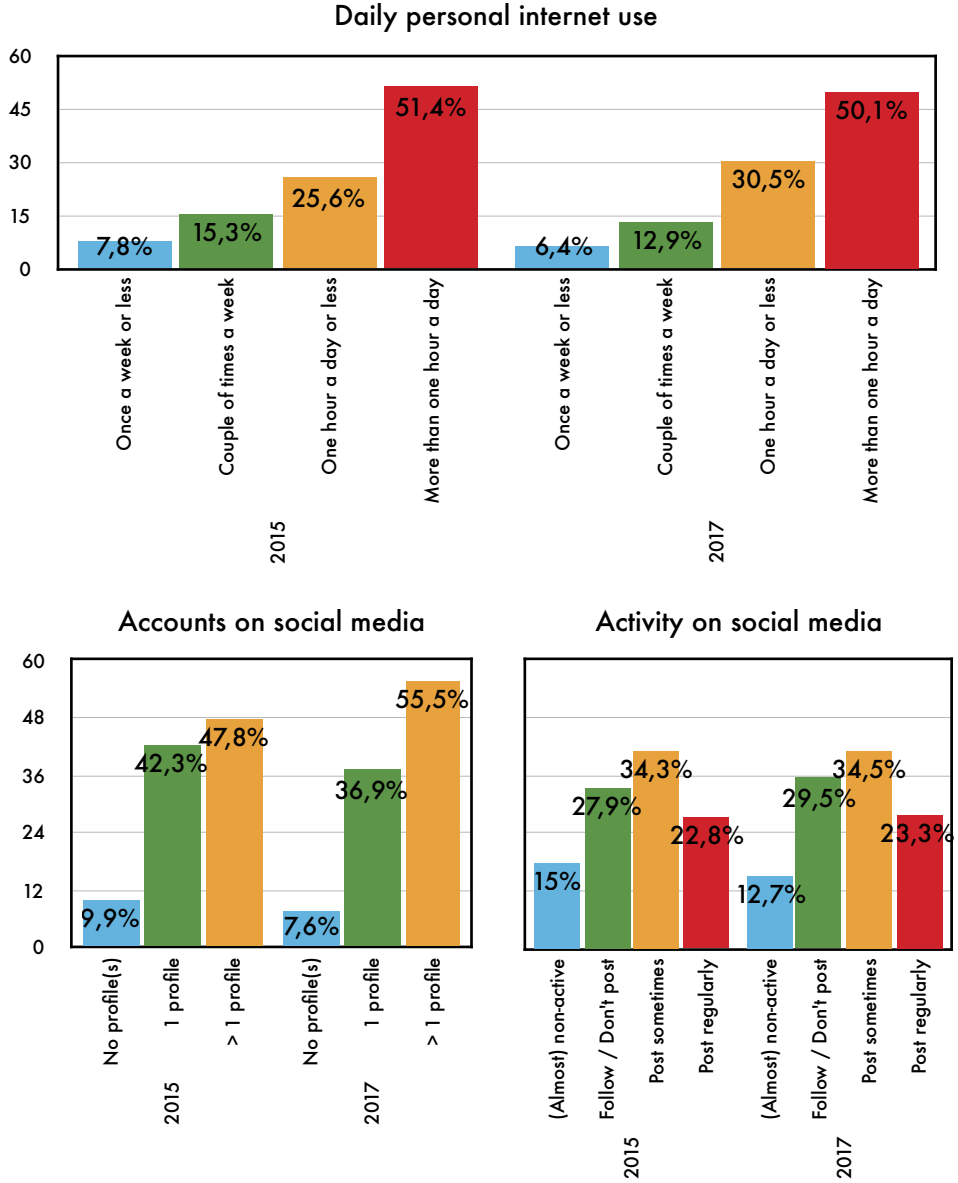


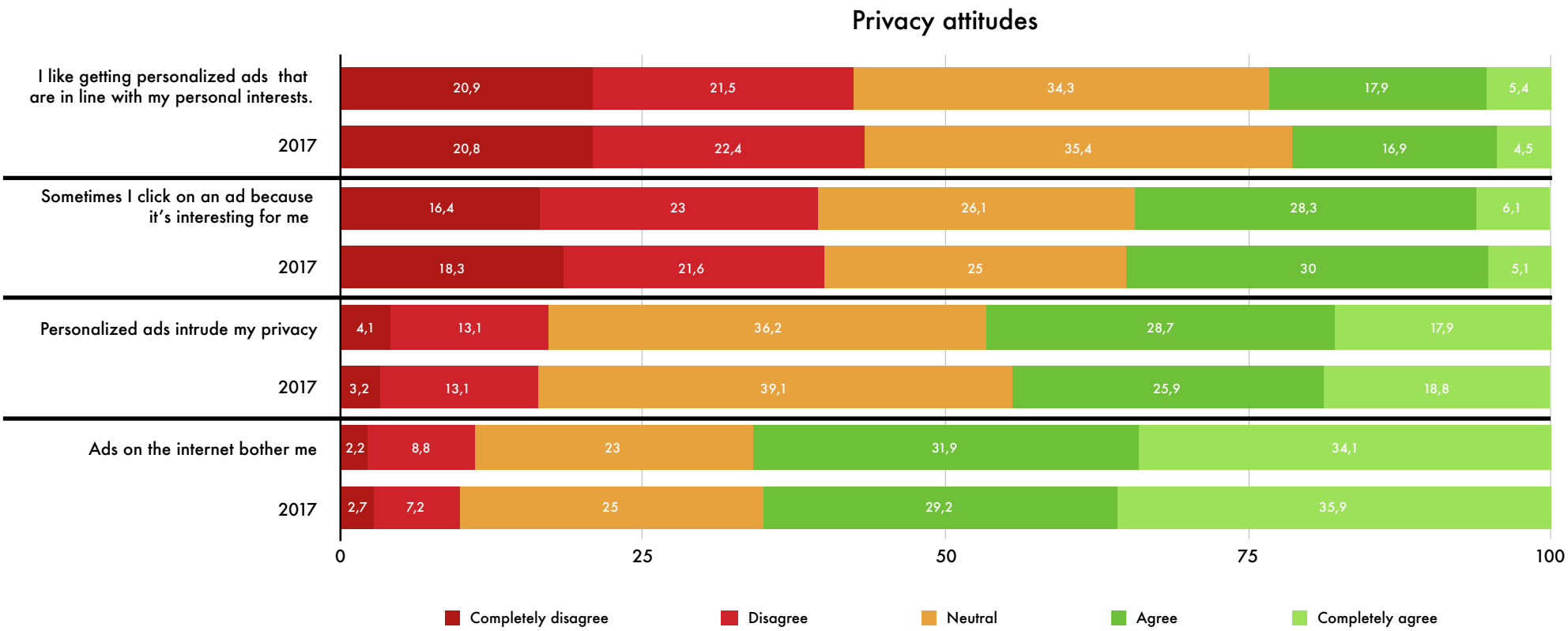


Some 35% post things every once in a while. 30% are "passive followers" and **13% are not active on social media**.

Even though the degree of activity on social media didn't change between 2015 and 2017, what did change significantly is the amount of profiles people have on several social media platforms ($p<.05$). Today, almost **56% reports to have several social media platforms** (compared to 48% in 2015).

While spending time online, young people of today almost inevitably get targeted by businesses that want to sell them things. Whether they like it or not (or are aware of it or not), based on their preferences, personal data or browsing history (cf. cookies), they receive widely varied sponsored content from a whole range of providers that have identified them as their "target population". **In our 2015 study, we found that our respondents generally reacted aversively to these commercial tactics. Based on these results, we would hypothesize that businesses have adapted their strategies in order to make their ads more in line with what their (potential) customers *actually want***. Thus, we would expect to see an evolution *in favor* of personalized ads. **However, this is not what we observe today, on the contrary**. We mostly observe a status-quo in how people feel about personalized ads. If we observe changes, they are mostly in the direction of people being less in favor of them, although they seem to click just a little more if a product interests them (although changes are small and significant only on the .10-level for "bothered" and "clicking on ad" only).





One quick methodological note before we start to zoom in on our key-concepts privacy knowledge, concerns, negotiation and action. In order to compare the 2015 and 2017 results, we follow the same data-analytical approach as then. This means that the "master-concepts" are measured by aggregating the responses on several sub-questions. This technique allows us to more reliably compare the two surveys and explore group differences in the concepts. When appropriate, however, we will still focus on the sub-questions that make up the scale of the concepts. In the text, we use stars to indicate different levels of statistical significance: 0,1-level (*) / 0,5-level (**) / 0.01-level (***). No indication of significance means no significant differences.

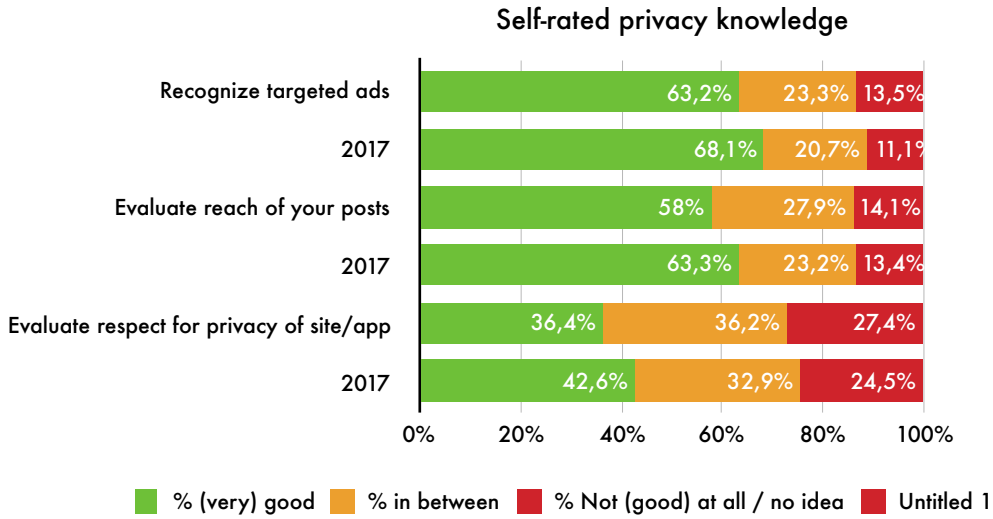
5. KEY PRIVACY CONCEPTS: RESULTS

5.1. PRIVACY KNOWLEDGE

In the 2015 survey, we found that, although young people seem to be quite aware (and concerned) about online privacy issues, a majority of the respondents feel that they don't have the adequate knowledge to cope with these issues. We observed a staggering 85% of the population that would like to know more about how to protect their personal information online with no significant group-differences, suggesting that this need for privacy skills was very broadly shared across the population.

Sadly, this can still be observed in our sample today. We notice no significant difference in people's desire and need for more privacy knowledge: **still 82% would like to know more about how to protect their personal information on the internet**. **This suggests that over the last two years, no real improvements have been made to educate people on how to protect their online privacy.** People still combine concerns with a rather limited knowledge, creating a possibly quite dangerous situation in which people don't feel that they are in control in managing their "private/public boundary". Only around 18% feels that they don't need extra information on how to protect their privacy.

What was rather striking in the 2015 study, was that, even though we observed this above finding, respondents generally **self-rated their privacy skills quite highly**. In our recent data, we can observe the same pattern with one notable difference. **We see a statistically significant improvement in how people feel they can evaluate the degree in which an app/website respects their privacy sufficiently** (**). The group that claims to be able to do this, grew from 36% to 43%. A possible explanation for this might be the increased emphasis on "privacy by default" in online services, in which the default setting is on increased privacy rather than "open for all". However, much more needs to be done, as this result also implies that **almost 6 in 10 people still *do not know* how to adequately assess the trustworthiness of apps/websites**. This number is in line with the above mentioned OECD study.



All the above questions referred to self-rated knowledge about privacy. We all know, however, that **people tend to overestimate their knowledge** on their privacy skills and knowledge. That's why we added 3 extra *factual* questions in the survey. The answers to these questions are factual. That is to say: there are "right" and "wrong" answers.

We asked three questions and the correct answer to all three of them is "not true". In the table below you can see the percentage of people who answered correctly to these questions.

Fact	2015	2017	Diff.
The law prohibits online services (such as Facebook, Twitter, applications, ...) to sell personal data to other companies.***	33,7%	41,9%	8%
	43,2%	38,1%	-5%
	23,1%	20,0%	-3%
Apps can never collect data on where I live if I never gave them my address.***	66,4%	69,1%	3%
	14,2%	17,2%	3%
	19,4%	13,7%	-6%
Apps almost never collect personal information about their users.***	73,9%	76,9%	3%
	8,6%	10,8%	2%
	17,5%	12,3%	-5%

Green = correct answer Red = wrong answer Orange = don't know

As you can see, in general, **objective privacy knowledge has significantly increased in the past 2 years**. We observe a large improvement of about 8% on first item. On average, the "no idea" category declined with around 5%, suggesting that **people have actually built up a better objective understanding of what businesses (can) do with personal data.**

Evolution and group differences in privacy knowledge

We constructed an aggregate measure of privacy knowledge based on exactly the same 5 items as in 2015 (see appendix), all of which refer to the self-rated knowledge that people report. For instance, one item looks at whether one can evaluate the reach of what one posts online while another one asks whether people know how they can change their privacy settings on social media. All these items form an aggregate (average) measure of privacy knowledge ranging from 1 (very low) to 5 (very high). **People estimate their privacy knowledge relatively high: the average in the 2017 sample is 3,7**.

Despite the ongoing attention for privacy issues, despite the fact that privacy has been an increasingly important policy topic, despite the fact that media coverage in the past 2 years about digital privacy doesn't seem to have subsided, we observe **no statistically significant shift in self-rated privacy knowledge among young Belgians (although we do see an improvement in objective privacy**

knowledge). There's still ample room for progress, especially when we think about the aforementioned alarmingly high number of people who feel like they should know more about how to protect their online privacy.

Focusing on group differences, this is what we observe today:

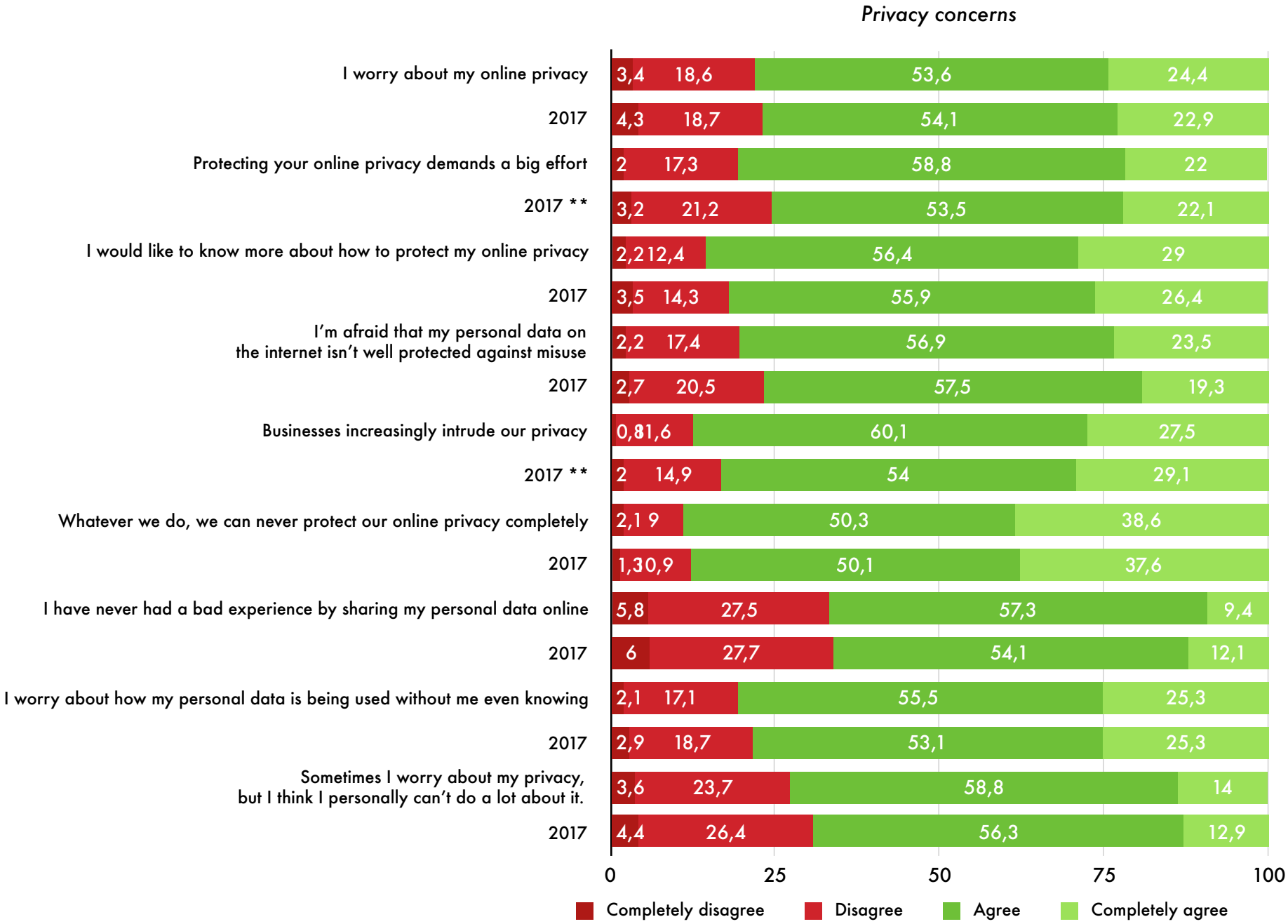
- Today, we still find that **younger people report higher levels of self-rated privacy knowledge****.
- The gender-divide in privacy knowledge, on the other hand, can't be observed in the 2017 sample: **men and who women report equally high levels of privacy knowledge**.
- In 2015, we found a significant correlation between intensity of internet usage and self-rated privacy knowledge. This link has diminished in the 2017 sample. However, the positive correlation between internet usage and privacy knowledge remains intact. The more hours one spends online, the higher the self-rated knowledge.
- A "new" group difference is that **French speaking Belgians report slightly higher privacy knowledge than Dutch speaking Belgians**.

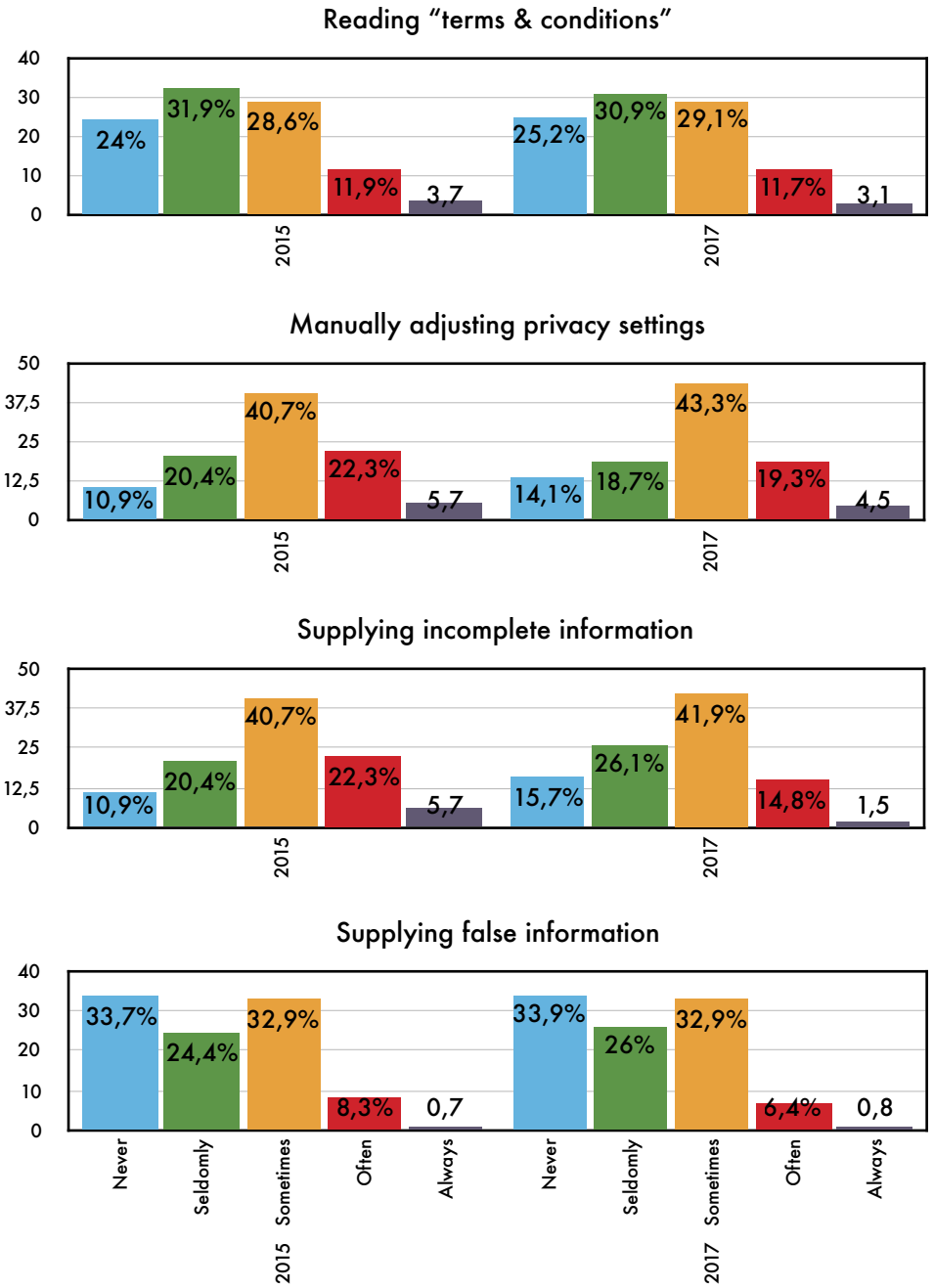
5.2. PRIVACY CONCERNS

Just like in 2015, we still observe **high privacy concerns in the Belgian population** under 40. Statistically speaking, there is not a whole lot to know about the differences in privacy concerns back in 2015 and now. In line with most of the other insights in the present survey, there **doesn't seem to be all that much of a shift going on**. Again, our data don't allow us to sketch a very cheerful picture on privacy concerns…

Today, **still almost 8 out of 10 worry about their online privacy. This number hasn't dropped since 2015**. Slightly more than 1 in 5 is not concerned. Still close to **80% of the Belgians worries about how their personal data is being used without them even knowing**. We don't see a drop in this number since 2015. *En plus,* respondents still feel as ignorant about protection of their personal information online as in 2015. **Almost 6 in 10 respondents claim not to know how to protect their personal data**. Only 5% is very confident that they know how to do this. **Fatalism still reigns** with more than 87% of the respondents convinced that whatever we do, we can never fully protect our online privacy.

We do see a **slight decrease in the number of people that feels like protecting their online privacy requires a lot of effort**. We also see a slight decrease in how convinced people are that businesses increasingly violate our privacy** (17% disagrees in 2017 versus 13% in 2015)**. Of course, this still means that more than 80% *do* feel that businesses increasingly intrude our privacy. There's work to do for companies to build up a credible relationship with their customers online. Being transparent and open about privacy and the use of personal data is one step in a good direction, as this will decrease the fatalism that people have about the "privacy black box" today.


Privacy concerns
I worry about my online privacy
3,4 18,6 53,6 24,4
2017
4,3 18,7 54,1 22,9
Protecting your online privacy demands a big effort
2 17,3 58,8 22
2017 **
3,2 21,2 53,5 22,1
I would like to know more about how to protect my online privacy
2,2 12,4 56,4 29
2017
3,5 14,3 55,9 26,4
I'm afraid that my personal data on the internet isn't well protected against misuse
2,2 17,4 56,9 23,5
2017
2,7 20,5 57,5 19,3
Businesses increasingly intrude our privacy
0,8 1,6 60,1 27,5
2017 **
2 14,9 54 29,1
Whatever we do, we can never protect our online privacy completely
2,1 9 50,3 38,6
2017
1,3 0,9 50,1 37,6
I have never had a bad experience by sharing my personal data online
5,8 27,5 57,3 9,4
2017
6 27,7 54,1 12,1
I worry about how my personal data is being used without me even knowing
2,1 17,1 55,5 25,3
2017
2,9 18,7 53,1 25,3
Sometimes I worry about my privacy, but I think I personally can't do a lot about it.
3,6 23,7 58,8 14
2017
4,4 26,4 56,3 12,9
0
25
50
75
100
Completely disagree
Disagree
Agree
Completely agree



Let's dive deeper into group differences in privacy concerns, and check whether concerns have significantly decreased.

Evolution and group differences in privacy concerns

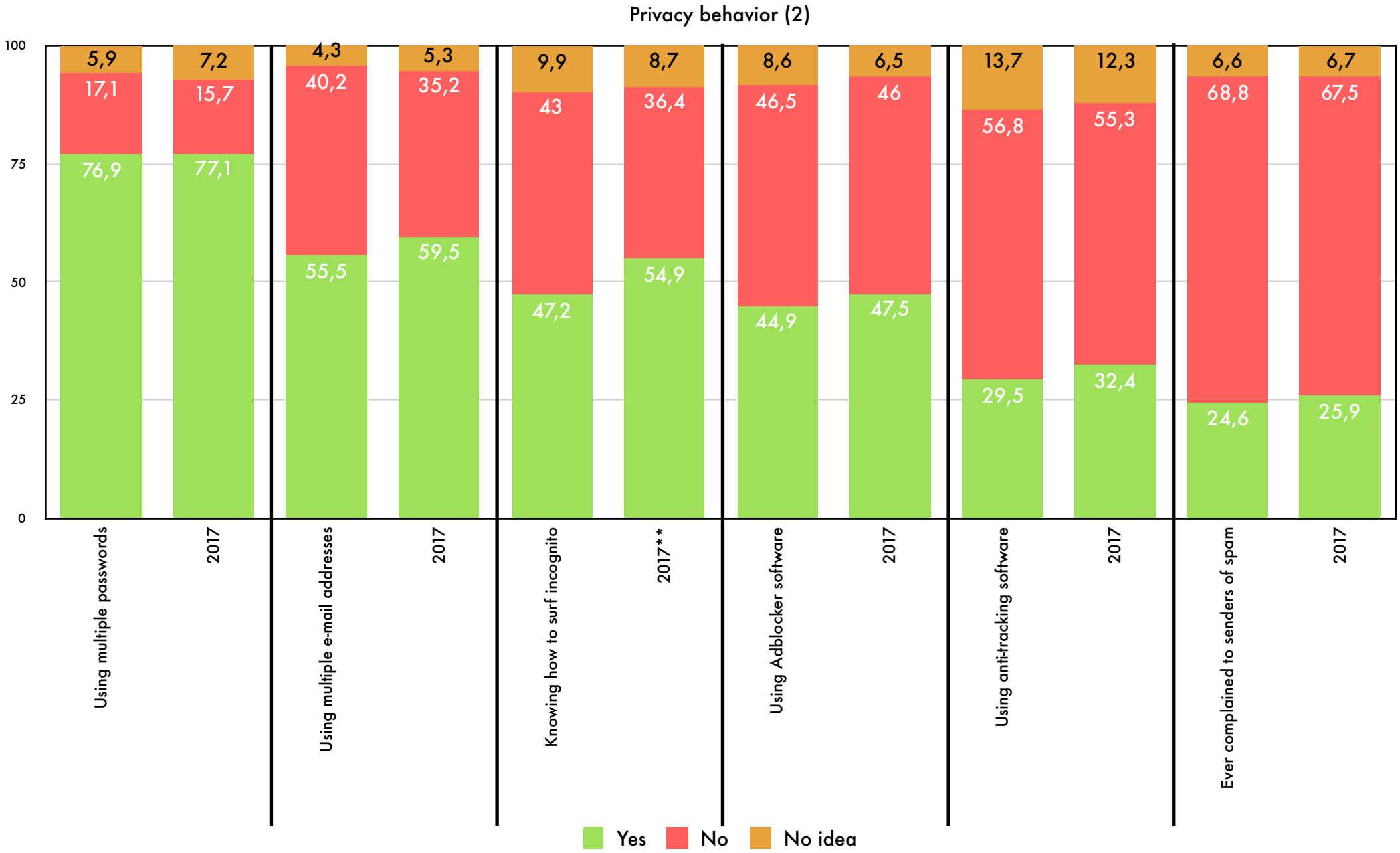
An independent t-test comparing the aggregated privacy concerns in 2015 with those in 2017, reveals no significant decrease in privacy concerns in Belgium. **Privacy concerns remain very high, the mean value on the 1 to 4 scale is 3,00**.

We could replicate the 2015 finding that **Wallonia is slightly more concerned than Flanders*****. Furthermore, the older age group (above 28) is a little more concerned than the younger group***. Just like in 2015, there are no gender differences in privacy concerns. Indeed: the finding that **concerns are quite generalized across social groups** still stands firmly in 2017.

5.3. PRIVACY BEHAVIOR

When we observe an increase in objective privacy knowledge (see above), does this mean that people are better aware of how to effectively protect their privacy online than in 2015? We confronted our respondents with 10 privacy enhancing behaviors and asked them if they used these strategies to protect their online privacy.

Again, no shift seems to have occurred in the past 2 years as no


Privacy behavior (2)
100
75
50
25
0
5,9
17,1
76,9
7,2
15,7
77,1
4,3
40,2
55,5
5,3
35,2
59,5
9,9
43
47,2
8,7
36,4
54,9
8,6
46,5
44,9
6,5
46
47,5
13,7
56,8
29,5
12,3
55,3
32,4
6,6
68,8
24,6
6,7
67,5
25,9
Using multiple passwords
2017
Using multiple e-mail addresses
2017
Knowing how to surf incognito
2017**
Using Adblocker software
2017
Using anti-tracking software
2017
Ever complained to senders of spam
2017
Yes
No
No idea

statistically significant changes in these behaviors can be found in the 2017 data.

When we're looking more closely to the second list of privacy enhancing behaviors, the same pattern emerges. There are no big differences between 2015 and 2017. Except for one: **people in 2017 have discovered the "private/incognito" browsing mode. 55% knows how to surf incognito (versus 47% in 2015)**.**

Among the most used tactics to protect online privacy are:

- **Using multiple passwords**: more than 3/4 of the respondents does this
- **Using multiple e-mail addresses**: almost 60%
- Installing **AdBlockers**: around 47%

Almost 1 in 3 uses more specialized anti-tracking software to protect their privacy. In other words: 1 in 3 has installed application(s) *especially to protect their privacy*.

Evolution and group differences in privacy behavior

When looking at the actions people take to protect their online privacy, we see a very slight decrease in this behavior, but this decline is not statistically significant. We conclude, therefore, that **no shift has taken place between 2015 and now. Privacy behaviors remained status-quo, which is in line with most of our other insights.**

What we didn't see in 2015 was a gender difference in privacy behavior. In 2017 we do see such difference with **men exhibiting a little more privacy behaviors than women** (*). We also see a regional difference popping up: Walloons take a little more action to protect their privacy than their Northern counterparts**. Lastly, we observe significant differences in actions between different professional groups (**) and education levels (*). Students take the most actions to safeguard their privacy, followed by clerks. Blue-collar workers and "other professions" show the lowest rates. Highly educated respondents tend to take more actions than others. The group that followed lower secondary education show the highest rates of privacy behavior (although reliability of this is probably rather limited, as only 33 people in this survey belong to this category).

5.4. PRIVACY NEGOTIATION

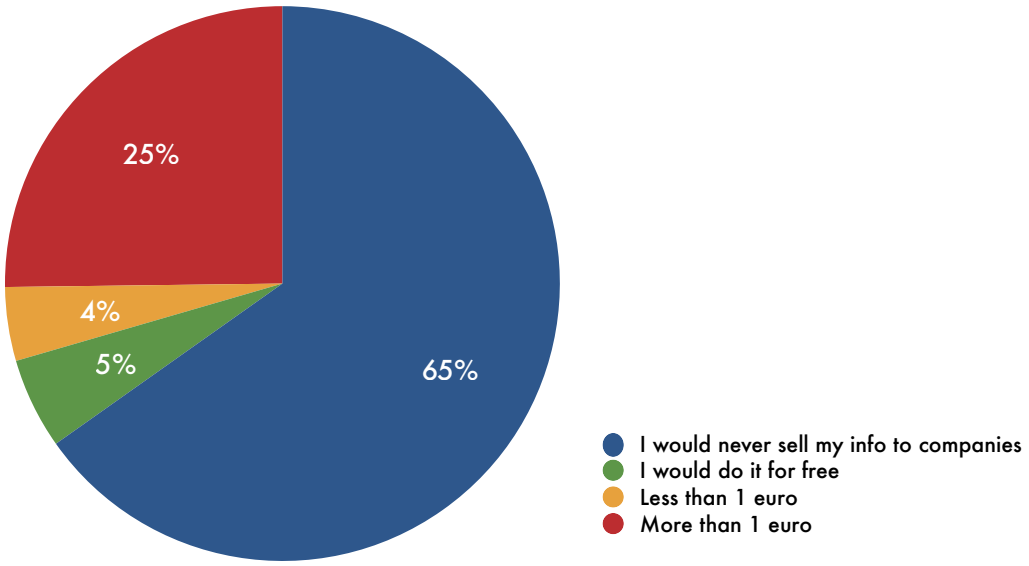
As we have seen and noted a couple of times, online privacy is a very slippery and often paradoxical domain. On one hand, we seem to be very concerned about abuses of our personal data and about violations of our boundary between public and private information. On the other hand, though, never in history have we given away so much intimate information about ourselves, our friends, our activities, our cultural, sexual and social preferences. As we noted in our earlier report, in many ways, what we do on the internet is an exchange in

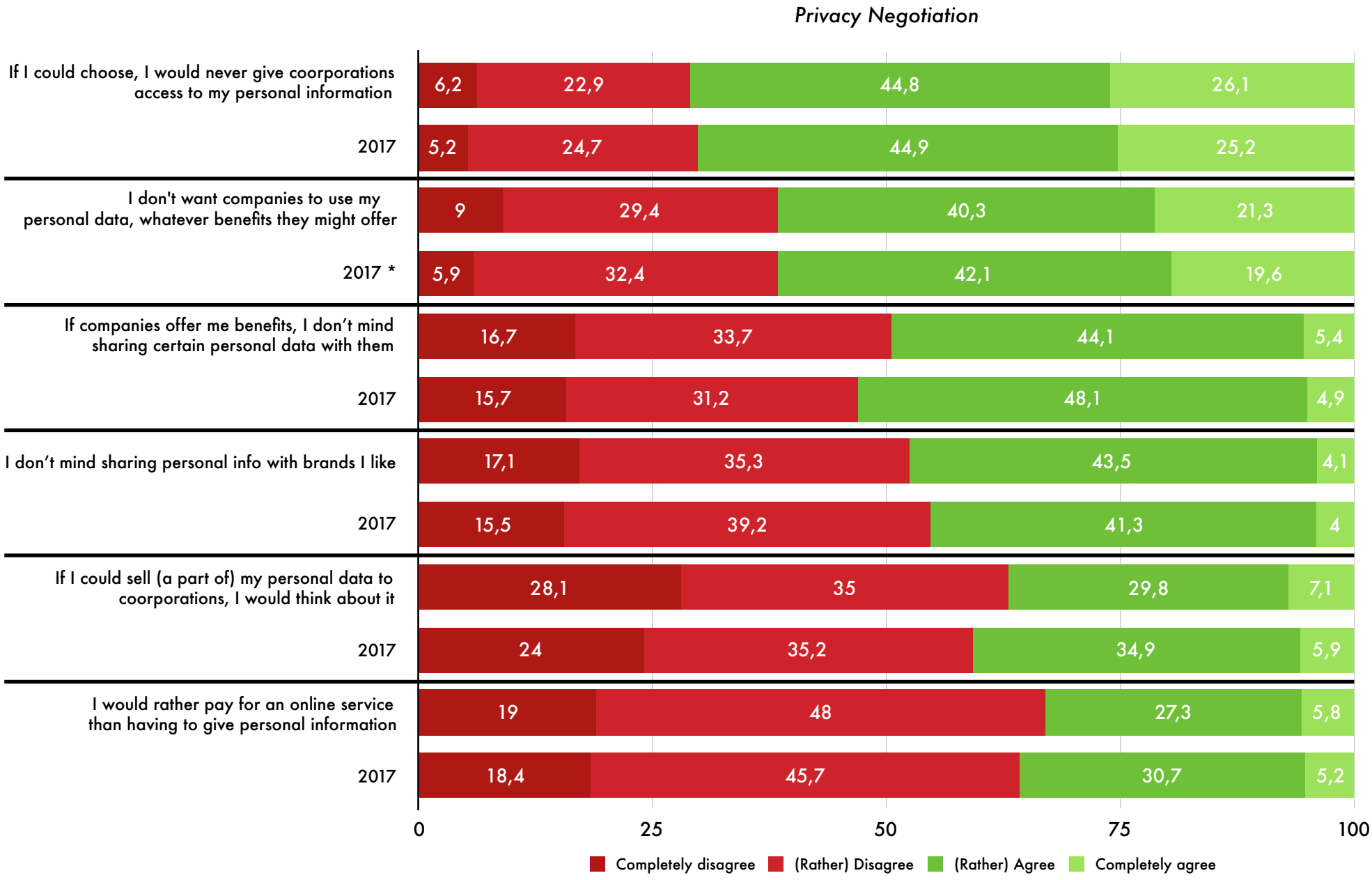
terms of personal data for a service (e.g. an account on Facebook). **Our personal data has become an economical asset in itself**. We all know how tempting it is to fill in some bits of personal information in order to win a contest or to become a user of a valuable online service. This is what we focused on again, today, after two years. Are young people willing to "pay" for services with their privacy? Do they consider this as good for them?

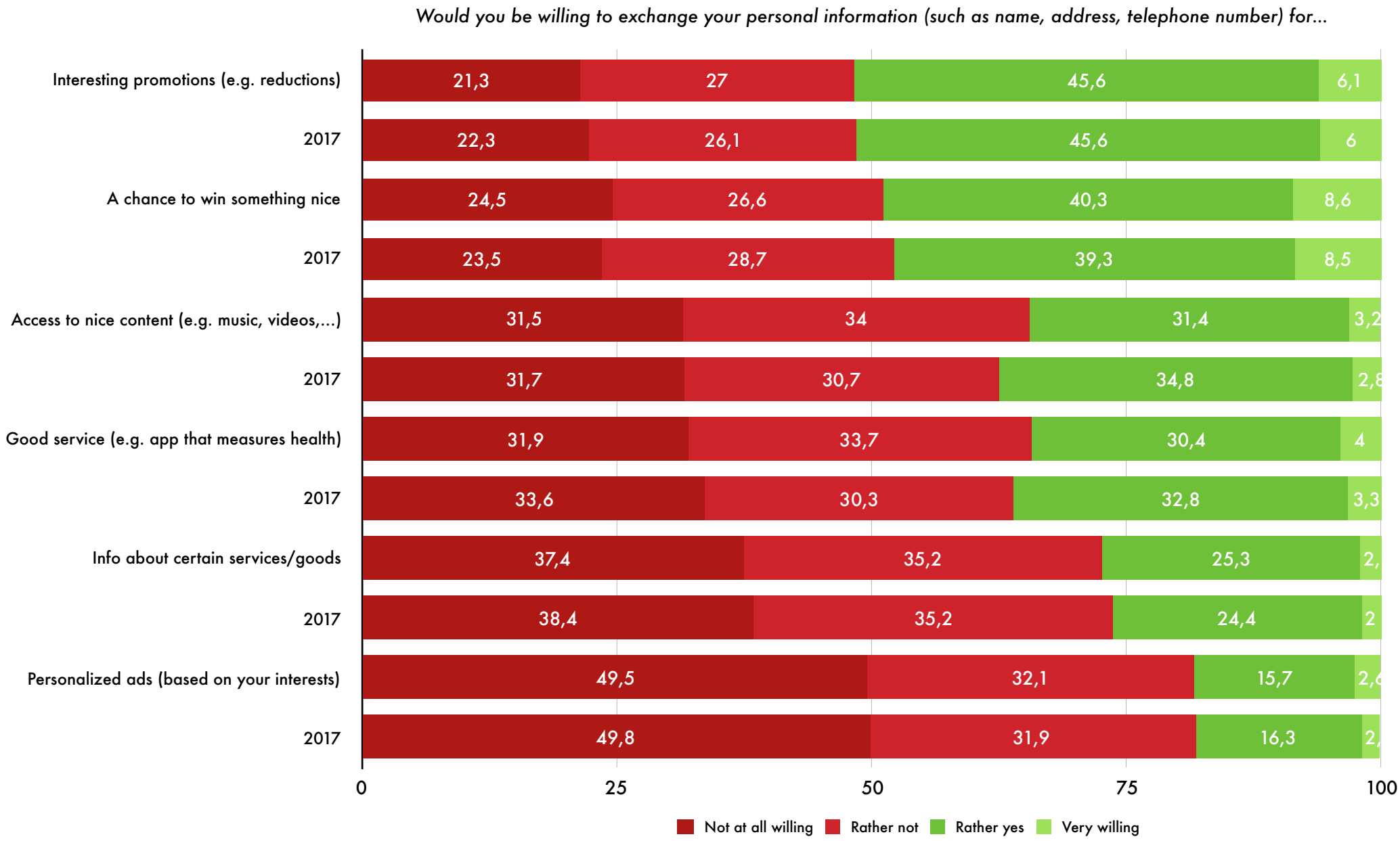
In 2015, when we asked our respondents whether they would exchange their personal information (defined as: all the information that they now share for free with their best friends on Facebook) to companies for cash money. Back then, around 7 in 10 claimed that they would never do this. This seemed to be in contradiction with the fact that *they already did this* with companies like Facebook, Amazon or whatever online retailer or service they used.

In our most recent 2017 data, we see a shift in this aspect of privacy negotiation. As the bigger piechart to the right shows, in comparison to the smaller one, **people today are slightly more in favor of selling their data to companies.** Around 1 in 3 agrees that their privacy has a price (read: can be bought by companies). This shift towards more willingness to negotiate their privacy is statistically significant on the . 05-level. As businesses of today increasingly find better ways to exploit people's private information, the willingness of the public seems to increase as well. A complete economical model is rapidly being build around personal data in exchange for benefits. Indeed, as

How much money would you want businesses to pay you in exchange for the information you now share with your best friends on Facebook?




Privacy Negotiation
If I could choose, I would never give coorporations access to my personal information
6,2
22,9
44,8
26,1
2017
5,2
24,7
44,9
25,2
I don't want companies to use my personal data, whatever benefits they might offer
9
29,4
40,3
21,3
2017 *
5,9
32,4
42,1
19,6
If companies offer me benefits, I don't mind sharing certain personal data with them
16,7
33,7
44,1
5,4
2017
15,7
31,2
48,1
4,9
I don't mind sharing personal info with brands I like
17,1
35,3
43,5
4,1
2017
15,5
39,2
41,3
4
If I could sell (a part of) my personal data to coorporations, I would think about it
28,1
35
29,8
7,1
2017
24
35,2
34,9
5,9
I would rather pay for an online service than having to give personal information
19
48
27,3
5,8
2017
18,4
45,7
30,7
5,2
0
25
50
75
100
Completely disagree
(Rather) Disagree
(Rather) Agree
Completely agree


Would you be willing to exchange your personal information (such as name, address, telephone number) for...
Interesting promotions (e.g. reductions)
21,3
27
45,6
6,1
2017
22,3
26,1
45,6
6
A chance to win something nice
24,5
26,6
40,3
8,6
2017
23,5
28,7
39,3
8,5
Access to nice content (e.g. music, videos,...)
31,5
34
31,4
3,2
2017
31,7
30,7
34,8
2,8
Good service (e.g. app that measures health)
31,9
33,7
30,4
4
2017
33,6
30,3
32,8
3,3
Info about certain services/goods
37,4
35,2
25,3
2,
2017
38,4
35,2
24,4
2
Personalized ads (based on your interests)
49,5
32,1
15,7
2,6
2017
49,8
31,9
16,3
2,
0
25
50
75
100
Not at all willing
Rather not
Rather yes
Very willing

we have heard so many times in the last couple of years: data is a very valuable resource and new models emerge to exploit this resource. However this is going to happen, it is going to be in negotiation. Like in the other key aspects of online privacy, **we can't observe a lot of significant evolutions in privacy negotiation. The numbers seem to have stayed rather stable over the last 2 years, suggesting that people still have the same online privacy attitude than 2 years ago.**

In general, we see several important issues when looking closer at the negotiation data:

- Although respondents don't want companies exploiting their personal data, **only 36% would we willing to pay (with money) for online services instead of paying with their personal information**. This is a little more than in 2015 (although this difference is not statistically significant).
- Around **4 in 10 respondents would be willing to think about selling some of at least some of their private information to companies.** We should note here that the distribution of this question is very bimodal: nearly 30% is absolutely not in favour of this. You could almost say that there seem to be "two kinds of people": those who would and those who wouldn't sell their data.
- In general, **people are aversive towards businesses and governments using their personal data**. 7 in 10 say that, if they could choose, they would rather not have companies/ governments looking into their personal information.

After these items, we asked the respondents whether they would be willing to exchange their personal information (such as name, address, telephone number, …) for a list of several benefits. These numbers stay in line with the numbers in 2015. We see the same pattern emerging again: **people are most willing to trade their personal information in exchange for interesting promotions (e.g. reductions) or a chance to win something nice**. Interesting content or good services can't inspire people to give away personal information. We note that **people are generally rather NOT willing to share too much information about themselves**: only around half of the population say they can be convinced to do this.

Businesses that seek to build up an online relationship with clients, should bear in mind that they have to start "below zero". People are very privacy concerned and not at all willing to share too much information about them. Businesses are always "intruders", and they should be aware of this in order to do it rightly. People find targeted ads annoying, and they don't like companies that use their data for their own benefit. People are also very unsure about what happens with their data. Companies that dare to be transparent about what they do with personal data of their clients will be appreciated more, as people probably also expect/suspect worse than what actually happens.

Evolution and group differences in privacy negotiation

In 2015, we found a significant difference in privacy negotiation between men and women. Today, we don't observe this difference anymore. Negotiation attitudes of men and women seem to have converged. Both sexes score on average around 2,35 on the scale from 1-4. The same holds true for the difference between Flanders and Wallonia. In 2015 Flemish people were a little more willing to negotiate a privacy exchange but this gap has been bridged. Walloons became a little more willing and Flemish respondents became a little less willing - they met in the middle at the same level of willingness to negotiate.

No statistically significant shift in privacy negotiation could be found in our current data compared to the 2015 dataset.

5. ACTION-CONCERNS PRIVACY TYPOLOGY

Now that we have sketched out the rough picture of the (lack of) evolution in privacy related attitudes and behaviors, it's time to check whether our privacy profiles still make sense today. We are interested in how the distribution changed. That is, we want to know if and how the 4 privacy clusters grew or shrank.

In this section, we follow the same strategy as two years ago. We do a cluster analysis based on the same two axes: privacy behavior and privacy concerns.

This results in 4 quadrants:
Low behavior / low concerns ("**Apathetics**")
Low behavior / high concerns ("**Mainstream**")
High behavior / low concerns ("**Fatalists**")
High behavior / high concerns ("**Privacy Priests**")

We note that when we say "low" of "high", we mean that they deviate from the *mean value* of the concepts in question. More correctly, we should then say "lower-than-average" instead of low. However, for reasons of convenience, we will stick with the terminology of the 2015 report.

Another important note is that, although we will identify clusters, **we should not overestimate the uniformity within these clusters**. We have a certain overlap between clusters. The types are thus a useful tool to look at our data in a simplified way, rather than fixed and clearly separated categories of people.

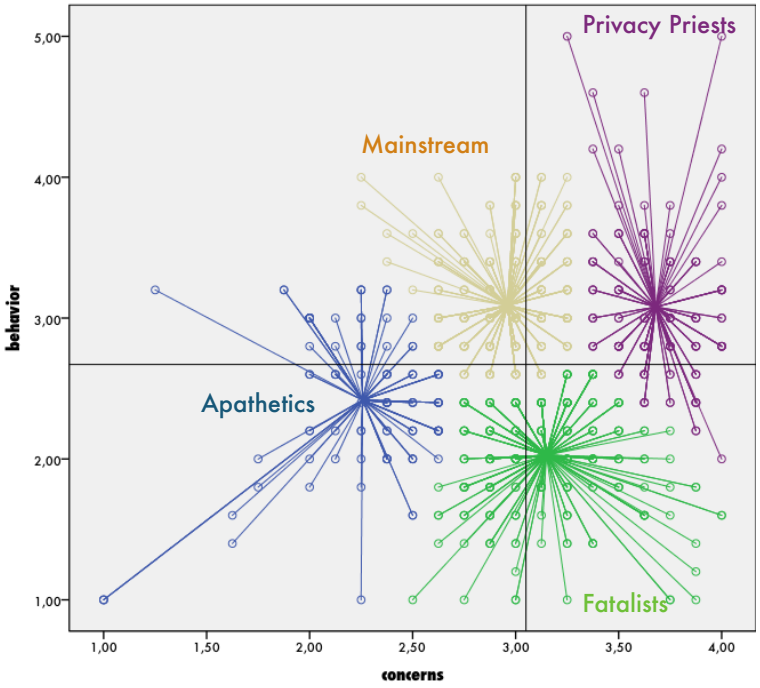
In the previous sections, the primary conclusion could be that, overall, few noteworthy "real" evolutions in attitudes and behavior towards online privacy can be observed. We have observed status-quo rather than change through time. This is, in itself, noteworthy. **It means that despite the ongoing attention for online privacy in the last two years hasn't really changed how people think and feel about it. Despite the intensification of reliance on data of new technologies, people's thoughts on privacy haven't quite as rapidly evolved.**

The previous sections mostly focused on separate variables. Now it's time to look at **how people "combine" these characteristics**. In other words, we're interested in the configuration of both privacy concerns and privacy behavior in clusters of people.

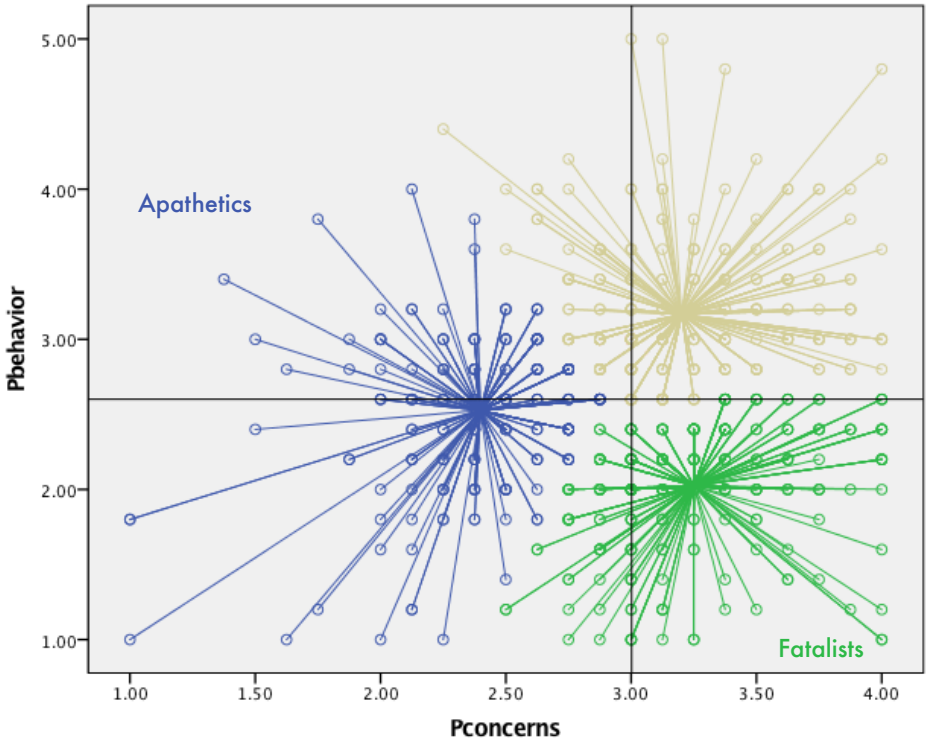
We executed the same cluster analysis on the new data[9]. We expected the four 2015 clusters to appear again, but **the clustering algorithm came up with only 3 basic clusters to best fit the data**. This might seem strange at first, seeing as we noticed few changes in privacy concern and privacy behavior. However, this cluster analysis is all about *combinations* of characteristics of respondents. In the previous sections, we always looked at separate variables. Here, we

[9] This was a two-step cluster analysis executed in SPSS. We let the algorithm decide on the best number of clusters to best fit the data we fed into it, just like we did in 2015.

shift our focus to how two variables are linked with each other. These variables in itself might not have changed significantly, the way they "come together" in individual respondents has.

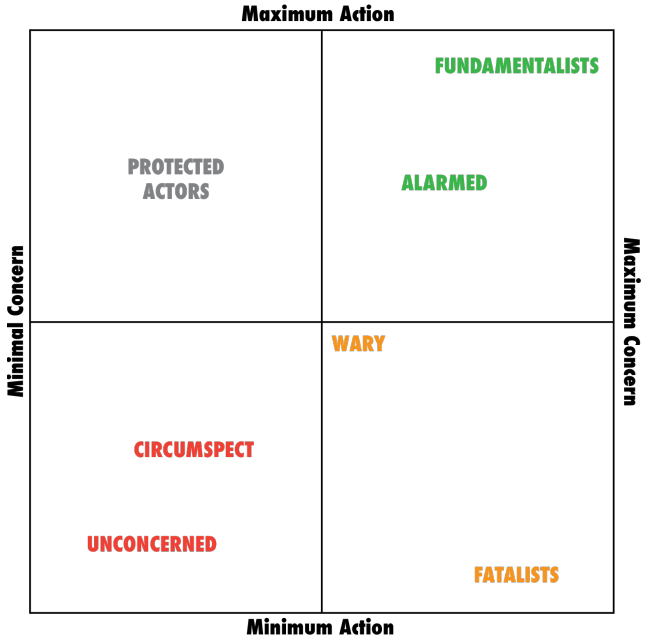


Concerned Actors



The three clusters that we find today, are more in line with existing privacy literature than the four clusters we found in 2015.

No cluster center is located in this quadrant. However: this quadrant contains a combination of Apathetics and Concerned Actors	**High concerns / High actions** **CONCERNED ACTORS (39%)** **Most concerned group, together with Fatalists** **Contains members of the 2015 Privacy Priests ànd Mainstream cluster.** **Lowest willingness to negotiate their privacy.**
Low concerns / Low Actions **APATHETICS (27%)** **Least concerned group, so they score the least on privacy-oriented behavior** **High willingness to negotiate their privacy.**	**High concerns / Low Actions** **FATALISTS (34%)** **Very concerned group but they do little to protect their online privacy** **Moderate willingness to negotiate their privacy.**



The above image shows the existing profiles based on privacy literature. In 2015, we added the "protected actors", which then turned out to be a large part of our "mainstream" group. Today, this quadrant remains, just like in the literature on privacy, more or less empty.

The cluster solution came up with 3 clusters instead of four. Using the terminology we used in the 2015 report, we could say that these are the three main groups:
Cluster 1: **Apathetics** (26,9%)
Cluster 2: **Fatalists** (34,4%)
Cluster 3: **Combination of Mainstream and Privacy Priests** (38,7%)

We will call the "combination" group "**Concerned Actors**", as it merges Privacy Priests with the old Mainstream group, who both scored high on behavior while scoring average to high on concerns. Privacy Priests, which consisted of 17% of the population, could not be observed *as a separate cluster* anymore. The 2015 Priests would now be embedded in the Concerned Actor group while those who had a Mainstream profile would be spread across different groups.

Our clusters are in line with existing literature. The Apathetics contain the "Unconcerned" and "Circumspect" groups from the scheme above. The Concerned Actors contain the "Alarmed" and the "Fundamentalists" and our Fatalists cluster could be compared with the combination of the "Wary" and "Fatalists".

Although the Mainstream group "vanished" into the other groups, a noticeable difference between the 2015 and 2017 clusters, is that all groups floated a little bit towards the center (where the average population scores on behavior and concerns are located). This suggests an increasing "homogenization" of privacy attitudes and behaviors. Of course, we still have 3 distinguishable profiles, but **there's an ever so small evolution towards homogenization of the profiles**. The terminology of 2015 can therefore seem a little bit exaggerated. "Apathetics" and "Fatalists" sound like extreme labels but the mere fact that almost around 1/3 of the population fits into these categories proves that they aren't so "extreme" as they sound.

The new clusters make sense, in the sense that the Mainstream group was actually a very "average" group that was located very close near the center of the behavior/concerns axes. This cluster in 2015 was a little bit "skewed" towards the first quadrant of low concerns and high actions. We speculated that this seemingly odd combination could be explained by the assumption that *because of their actions, the mainstream group wasn't really concerned*. Today, it seems like the **Mainstream cluster has "bled into" the other 3 clusters that have a more "logical" combination of concerns and behaviors. The new clustering solution leaves the first quadrant filled only with little parts of the Concerned Actors and the Apathetics. We can clearly see that the centers of the clusters are each located in their "own" quadrant, the Fatalists being the most "isolated" group.**

Let's explain the three clusters in more detail…

Apathetics combine lower than average concerns with lower than average actions. They are the ones that just don't care all that much about their online privacy. They are not very alarmed and as a consequence don't see the need to constantly take measures to protect their privacy. They score significantly lower than the other two profiles on privacy negotiation (see further) but rather high on self-rated privacy knowledge. In short, they think they know what there is to know about online privacy, but they just do not care about it for themselves.

Fatalists are more than averagely concerned about their online privacy but they do little to protect their online privacy. They are the group that is most in need of privacy education as their self-rated privacy knowledge is the lowest of all three groups (see further). They are in the unhealthy situation of a certain powerlessness: they are concerned but feel they can't do anything about it anyway. They don't feel empowered to safeguard their online privacy and as a result they relinquish control and have the feeling that it doesn't matter anyway.

Concerned Actors consists of a part of the 2015 Mainstream cluster and a part of the Privacy Priests cluster. They are the largest cluster (39%) and feel more concerned than average about their online privacy. Unlike the Fatalists below them, they are the ones that do take measures to protect their online privacy. They are less than others willing to negotiate deals with businesses that involve their personal information, but they are always wary about potential misuses or abuses of that deal.

5.1. Group differences in privacy profiles

In 2015, we learned that privacy profiles do not follow clear socio-demographic demarcation lines. We re-examined this finding and find new evidence of this. In this section, we are interested to see whether some profiles are over- or underrepresented in certain socio-demographically defined groups.

We find significant differences in the distribution of privacy profiles in the following groups:

- **Region***:** Apathetics are overrepresented in Flanders. In Flanders, 34% belongs to the Apathetic group, whereas in Wallonia this is only 20%. Wallonia also has more Concerned Actors (44%) versus Flanders (34%). A speculative explanation for this North-South gap is a differential media coverage about privacy.
- **Professional status*****: students are more likely to belong to the Concerned Actor group compared to the others (46%). They also are, together with the self-employed category, more likely to belong to the Apathetics group.
- **Profiles on social media**** : People without any profiles on social media are most likely to be in the Concerned Actor group (40%). This seems logical, as concerned people could be thought to avoid social media platforms that are known to intrude privacy to a certain extent. They also are least likely to be Apathetics (16% versus 27% in the global population).
- **Age group*****: Even though there are no differences in the number of Concerned Actors in the two age groups (both around 39%), people older than 28 are less likely to be Apathetics (23% vs. 33% in the younger group) and more likely to be Fatalists (38% versus 28%).

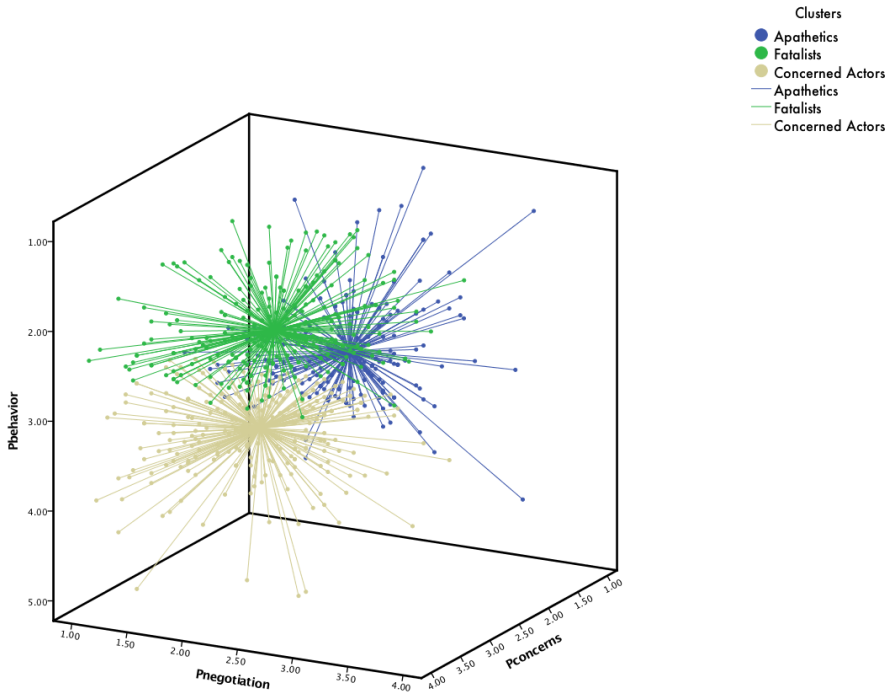
We couldn't observe sex differences or differences in profiles depending on internet use or intensity of activity on social media.

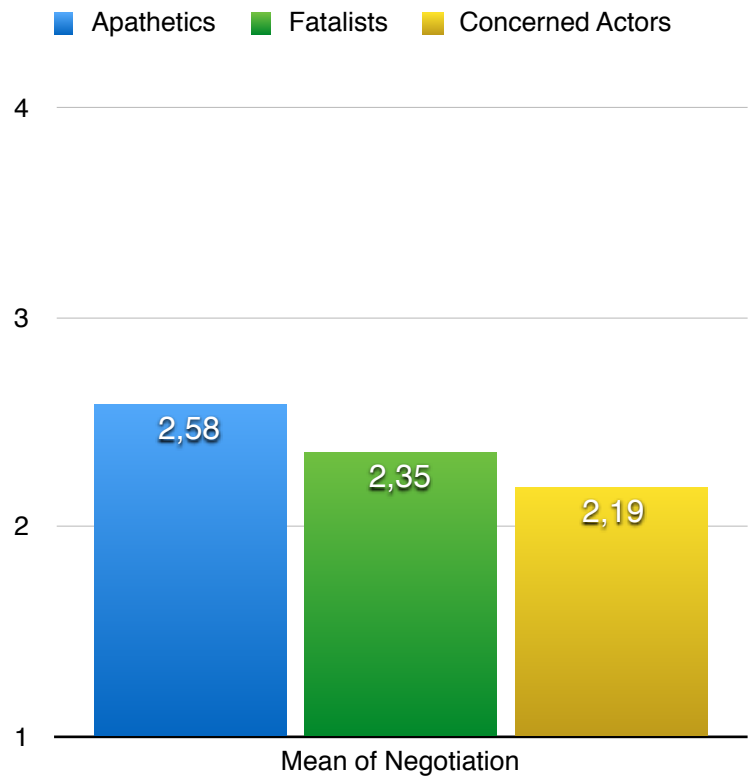
5.2. Privacy profiles and privacy negotiation & knowledge

How should different privacy profiles be scored in terms of how willing they are to negotiate or exchange their personal information for certain benefits? The 3D figure plots out the three privacy profiles together with privacy negotiation. The image reveals visibly that although the clusters overlap, the **centers of the clusters do score differently on the privacy negotiation axis**. **More in depth analysis, shows that the clusters indeed differ significantly (p<. 001) in their willingness to negotiate their privacy**. It is as would be expected: **Concerned Actors score the lowest on privacy negotiation, Apathetics score highest (average of 2,58 on the 1 to 4 scale).**

We repeat that there is a high resistance to privacy negotiation in the general population. People in general are not very willing to trade very much of their personal information in exchange for benefits. **If there is one thing that is of central importance, it is that people themselves know and can control what they share / what is being used by companies**. The "threshold" of what individuals find acceptable to trade in exchange for benefits greatly differs in the population (some people do not mind sharing their personal pictures publicly while others don't even want their full name listed anywhere). Choice and transparency is of crucial importance. Not surprisingly, Apathetics are most in favor of negotiation but it still should be noted that they "only" score 2,58 on a 1 to 4 scale so concluding that this group is "very willing" to exchange their information for benefits would be exaggerated.

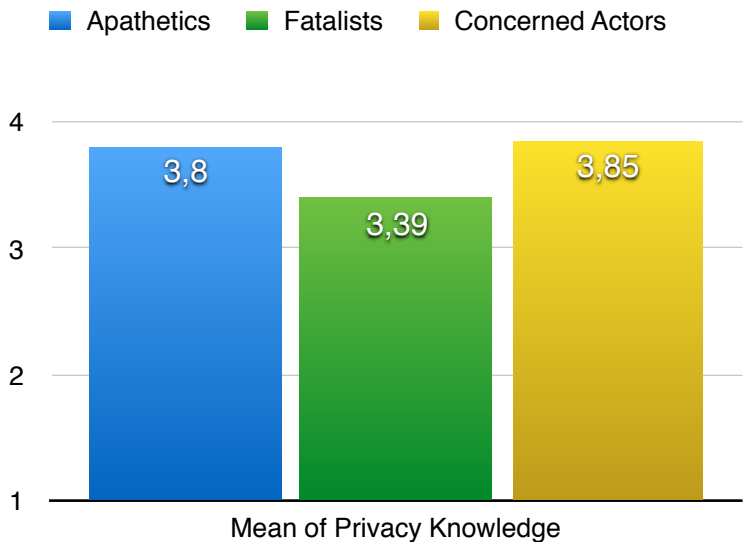
Along with cluster differences in privacy negotiation, were were interested to see if privacy knowledge is also distributed unevenly across the privacy typology (something we didn't discuss in depth in the 2015 report). We find today that there are indeed significant **differences in privacy knowledge between the different clusters.**





We find that Concerned Actors rate their knowledge of online privacy the highest and Fatalists rate it the lowest. Important side-note: the objective privacy knowledge of the respondents (the 1 to 3 rating based on the 3 factual privacy questions) is *not* significantly different from cluster to cluster, **suggesting objective and self-rated privacy knowledge is something different altogether. Indeed, we find a significant but rather weak correlation (r=0.107) between the two concepts.**

The persistence of significant cluster differences in knowledge and willingness to negotiate privacy, suggests that, depending on cluster membership, people expect/need to be approached differently. Levels of resistance to companies that use personal data, differ between the three privacy profiles. Different communication strategies are needed to address the needs of the different profiles. For instance, an online marketing campaign could be very good for brand engagement amongst the Apathetics. The same campaign, however, could be detrimental for the brand amongst the Concerned Actors. A good understanding of how different people feel about their online privacy would greatly benefit companies and the effectiveness of their communication strategies.



6. CONCLUSIONS

In this study we compared 2015 insights on online privacy with the insights gathered from the same survey questions in 2017. The primary conclusion could be that, overall, few noteworthy "real" evolutions in attitudes and behavior towards online privacy can be observed. **We have observed status-quo rather than change through time**. This is, in itself, noteworthy. **It means that despite the ongoing attention for online privacy in the last two years hasn't really changed how people think and feel about it**. Despite the intensification of reliance on data of new technologies, people's thoughts on privacy haven't quite as rapidly evolved.

There's still a lot of work that needs to be done. Firstly, privacy knowledge hasn't changed in the last 2 years. Despite the ongoing attention for privacy issues, despite the fact that privacy has been an increasingly important policy topic, despite the fact that media coverage in the past 2 years about digital privacy doesn't seem to have subsided, we observe **no statistically significant shift in self-rated privacy knowledge among young Belgians (although we do see a small improvement in objective privacy knowledge)**.

People are still as concerned as they were when it comes to their online privacy. **They still feel like online privacy is a big black box that they can't really control.** They don't know what online businesses and governments do with their data and they dislike this very fact: the lack of transparency. This makes sense. A lot of people are not categorically refusing to exchange their privacy for certain benefits… But they want to make a conscious choice for themselves. Privacy in the digital era has shifted from an absolute human right, something that was fixed, to a more flexible concept. **Online privacy today means navigating through a complex online landscape, evaluating who and what to (dis)trust, and making conscious and well-informed choices about what you allow other people to do with your data.**

We have seen that there are different groups of people that differ in their vision on (their) privacy. In 2015, we found 4 privacy clusters: Mainstream, Fatalists, Apathetics and Privacy Priests. Today, we only find 3 clusters. **The most significant shift is that the group of the Privacy Priests and the Mainstream have merged to form a new group which we chose to call the Concerned Actors.** These groups differ along socio-demographic lines (for instance, Dutch speaking Belgians are more likely to be Apathetics and people between 28 and 40 are more likely to be Fatalists) but also in their willingness to exchange their privacy for benefits. Apathetics and Fatalists are the most interesting groups for businesses that make use of online personal data. The problem, however, is that these groups generally do not *like* to give away their personal information. They view this more as a negative choice: something they are rather "fatalistic" about because they feel powerless anyway.

People aren't always against companies using their personal data, but they need to feel in control. They want to know what you do with the data, how you use it, if you sell it, what you know about them, and so forth. The more transparent you are about your (actually, *their*) data, the higher the trust will be. When we asked the respondents to openly comment on this survey, this came out very clearly. It's the "mystery" around (the lack of) online privacy that creates the suspicion. People would very much like to know what others know about them and how this is being used. **They want to stay in the drivers seat to assess and adjust the data that some companies have on them.**

2017 is not very different from 2015: there hasn't changed a lot. This does not mean that we should stop our efforts to educate citizens/consumers about online privacy. And **it shouldn't stop us from adapting our business strategies to the persistent and unhealthy situation of high concerns and high feelings of powerlessness regarding online privacy.** A staggering majority of the people claim they want to know more about how to protect their online privacy. This means two important things:

1) People feel like they don't know enough about online privacy
2) People feel like they don't take enough action to protect their online privacy

Among the institutions that are often cited as "trusted businesses" are banks. Of all the items we listed, people were least willing to share their financial data with businesses (even less so than their medical records!). Only 10% would be willing to share this information in return for certain benefits (almost twice as many would exchange their medical information). People share this sensitive information with their banks, which is why they rank among the highest in trust.

Using this privileged position, banks and other trusted institutions such as governments and specialized non-profits, could possibly play an important role in educating online privacy and enhancing privacy skills in the general population. We have seen that it is clearly not a thing that (only) the educational system can be made responsible for, as we are talking about a majority of people that already left the educational system.

The digital revolution is a very recent phenomenon and it should come as no surprise that our cultural system (which contains attitudes, concerns, fears, hopes, …) lags behind the technological evolutions we have seen in the past years. We're slowly adapting to a new world that reshaped our whole notion of privacy. It will take time and as we have clearly been able to underline in this research, we observed a certain persistence of cultural values/feelings about privacy over the short period of 2 years. It's important to keep monitoring these feelings, as it will guide our new strategies to be better in line with what people really want.

We have shown that in two years time, not much changed in how people feel and act with regard to online privacy. This means that their concerns and lack of knowledge/skills have not been adequately addressed. It is clear that there are enormous **opportunities** here.

APPENDIX

PRIVACY CONCERNS **(Cronbach's Alpha = 0.84)** **(Strongly agree - Agree - Disagree - Strongly disagree)**	
I worry about my online privacy	
Protecting your privacy on the internet requires a huge effort	
I would like to know more about how I can protect my personal info on the internet	
I'm afraid my personal online data is not well protected against misuses	
I'm worried about how my personal data is being used without my knowledge	
Corporations increasingly violate our privacy	
Whatever we do, we can never fully protect our online privacy	
I'm worried about my online privacy, but I think I personally can't do a lot about that	
PRIVACY BEHAVIOR **(Cronbach's Alpha = 0.66)** **(Never - Seldom - Sometimes - Often - Always)**	
If I sign up for an app/site, I read their "terms & conditions" in advance.	
I manually set up which personal data an app/site can collect about me	
I fill in incorrect personal information if I register on a company's website	
I fill in incomplete personal information if I register on a company's website	
I make sure that the things I post on the internet can not be seen by the wrong people	
SELF-RATED PRIVACY KNOWLEDGE **(Cronbach's Alpha = 0.86)** **(How well can you do the following things? Not at all <-> Very well (5 point scale))**	
Change your privacy settings on social media	
Evaluate if a website is trustworthy	
Recognise advertisements that are based on your personal internet history	
Evaluate who can see what you post online	
Evaluate if a website/app respects your privacy	
PRIVACY NEGOTIATION **(Cronbach's Alpha = 0.72)** **(Strongly agree - Agree - Disagree - Strongly disagree)**	
If companies give me benefits, I don't have any problems with sharing certain personal information with them	
I don't have problems with sharing personal information with brands that I like	
(Recoded) I don't want companies to use my personal data, whatever the benefits they offer me	

PRIVACY NEGOTIATION **(Cronbach's Alpha = 0.72)** **(Strongly agree - Agree - Disagree - Strongly disagree)**	
(Recoded) I would rather pay for an online service than having to give them personal information	
(Recoded) If I could choose, I would never give companies access to my personal information	
If I could sell (a part of) my personal data, I would consider to do so	

Descriptive statistics

	Mean 2015	Mean 2017	Range	St.Dev
KNOWLEDGE	3,48	3,63	1-5	0,83
CONCERNS	3,05	3,00	1-4	0,50
BEHAVIOR	2,67	2,60	1-5	0,66
NEGOTIATION	2,33	2,35	1-4	0,53