

#Delete Cyberbullying  

Teacher's Manual

Index

Introduction : presentation of the #DeleteCyberbullying app	3
Suggested use in the context of a lesson or activity about cyberbullying	3
How to use this manual	3-4
In class activities and lesson plans	5
Activity 1 : what is cyberbullying ?	5
Activity 2 : what's so special about cyberbullying ?	7
Activity 3 : consequences of cyberbullying	9
Activity 4 : what should you do in case of cyberbullying ?	10
Activity 5 : privacy online, why bother ?	12
Activity 6 : how does the internet work ?	13
Activity 7 : the internet of spam, scam and advertising	18
Annexe 1 : full list of the #DeleteCyberbullying app questions	25
“Test your knowledge” questions	25-29
“How about you?” questions	30-31
Annexe 2 : article about the consequences of cyberbullying	32
Annexe 3 : articles about privacy	33-36
Annexe 4 : 10 tips on protecting your privacy online	37
Annexe 5: How does the internet work?	38
Annexe 6: Business models for online services	39
Annexe 7: Online advertising, spam and scam	40
Credits and sources	41
Additional information	42
Licence	43

Introduction: presentation of the #DeleteCyberbullying app

The #DeleteCyberbullying app is an interactive quiz for teenagers, parents and teachers that displays customized feedback based on the responses to the quiz. The aim is to redirect the user to the most relevant information sources, material or even to be able to call for help if the user is experiencing cyberbullying.

The feedback will also be automatically customized according to the users' language and country, in partnership with local organisations working on the issue of cyberbullying.

It is available for Android since June 2014 and for iOS since November 2014. The initial release of the app covered the following countries (including the native language of the country): Belgium, France, United Kingdom, Ireland, Netherlands, Finland, Denmark, Greece, Bulgaria, Spain, Croatia, Germany, Sweden and Hungary.

Other features of the app include:

- An integrated awareness raising video about cyberbullying.
- A "one touch" button for help in case the user is in need of direct assistance.
- Information about the project and a "What's New" section to keep up to date with the latest news of the Delete Cyberbullying project.

The aim of our project is to ensure that the app is massively downloaded and used by teenagers (mostly between the age of 12 to 18), parents and teachers to raise their awareness about the issue, contribute to prevent cyberbullying and serve as a unique portal to access information about cyberbullying in the users' country and language to get direct help if needed.

The app is available in the following languages: English, French, German, Spanish, Finnish, Hungarian, Bulgarian, Dutch, Croatian, Greek, Swedish and Danish.

Suggested use in the context of a lesson or activity about cyberbullying

It is recommended to encourage your students to download the app and use it for a few days before the intended lesson or activity. Students should take the "how about you?" quiz once, and take the "test your knowledge" quiz at least three times to ensure they get a sufficient pool of different questions.

Students should also write down three comments, remarks or questions they may have or topics they would like to discuss vis-à-vis the app quizzes. During the lesson, students will be invited to share their thoughts with the rest of the class.

How to use this manual

This manual comprises of a set of activities or lessons on specific issues related to cyberbullying. They can either be directly related to cyberbullying (definition of cyberbullying, how to react...) or indirectly (privacy protection, digital skills...) The activities or lessons are modular and can be used independently in order to shape the overall lesson in class according to the interests, comments and questions from students. It is recommended however to start with the first activity on the definition of cyberbullying.

The activities/lessons serve mainly as a general guide and are not intended as a comprehensive lesson plan on cyberbullying. The app and the full list of questions can in and of itself serve as a “lesson starter” after which the teacher can draft his/her own lesson plan.

Each activity/lesson will include:

- some indications as to the questions in the app that it relates to (see the full list of questions in the annexe),
- some indications related to timing and target age groups,
- other activities/lessons that need to be discussed with students beforehand (pre-required activities),
- other activities/lessons that are related and could be developed in parallel or at a later stage,
- a short summary of the relevance of the activity/lesson for students and what they are expected to learn.

Activity 1 : what is cyberbullying ?

Related app questions: question 1 from the “test your knowledge” quiz.

Timing: 15 minutes.

Age group: 10-18 year olds.

Homework: none.

Pre-requisites: none.

Related activities: activities 2 and 3.

Objectives: to develop a general understanding of cyberbullying, its characteristics and be able to identify it if/when students see/experience it.

Paper version:

Ask the students to take a sheet of paper and write down what they believe are the four characteristics that define cyberbullying. (2 minutes)

Call for volunteers or handpick students to read out their contributions and summarize/group the main ideas on the board. (6 minutes)

At that point, ask whether any student believes some element is missing from the characteristics list on the board. (2 minutes)

Use the remaining time to complement or comment on the characteristics that students came up with on the basis of the characteristics below. (5 minutes)

Online digital version:

Create a Google Docs form with the question “With a few key word, what are according to you the main characteristics of cyberbullying?” (prior to the lesson)

Share the link with students and ask them to fill in the form with their answer. Export the Google doc content and paste it into a word cloud service such as “Wordle”.
<http://www.wordle.net/create> (3 minutes)

Project the word cloud on the white board and ask students to discuss what they see, for instance, what the most recurring words are and whether anything is missing from the list. (7 minutes)

Use the remaining time to complement or comment on the characteristics that students came up with on the basis of the characteristics below. (5 minutes)

Cyberbullying has many different "official" definitions. Although definitions differ, there are a series of descriptors for bullying and cyberbullying that can be identified:

- Firstly, the concept that the perpetrator **intends to hurt the target**, whether emotionally or physically.
- Second, there is an **imbalance of power** between the perpetrator and the victim. This is easily identifiable for traditional bullying but is harder to define when it comes to the online world. The fact that the bully or bullies remains often anonymous and the power that the bully or bullies has/have when it comes to reaching nearly instantaneously a wide audience with embarrassing or hurtful material can be a proof of this imbalance of power.
- Third, there is always an element of **repetition or continued threat of further aggression**. Cyberbullying and/or bullying are not one-off comments or threats, that could be rather defined as "flaming"¹, "trolling"² or simply one-off aggression. One has to be careful however, since in the online world, a "one-off" aggression from multiple users or from a single user but massively shared by other users becomes effectively cyberbullying.
- Finally, the most obvious characteristic of cyberbullying is that it involves **information and communication technologies** (such as smartphones, computers, tablets...) and especially the **internet**.

It is worth mentioning that **differentiating cyberbullying from sexual harassment, cyberstalking and other behaviours is very difficult**. Cyberbullying can be carried out in the form of sexual harassment, for instance by commenting the body, appearance or sex/gender, forwarding intimate pictures (sexual content, naked body/body parts) or videos, spreading sexual rumours etc. All of these actions can be understood as both cyberbullying and sexual harassment.

The distinction, however, is less important than to recognise that the **ultimate effect** can be very much the same (see activity 2 on the consequences of cyberbullying) and therefore the resulting steps to be taken by the victim remain mostly the same (see activity 3 on how to react to cyberbullying).

¹ http://en.wikipedia.org/wiki/Flaming_%28Internet%29

² Many terms such as "trolling" or "flaming" are in their infancy and can take various meanings according to the different cultural setting. Trolling is akin to cyberbullying in some instances. Flaming is usually understood as an outburst of hate and aggressiveness on chat forums or social networks, often on controversial topics. Trolling is usually understood as the action of initiating discord by starting arguments or upsetting people. Des Butler, Sally Kift & Marilyn Campbell, "Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?", *eLaw Journal: Murdoch University Electronic Journal of Law*, Vol 16, No 1 (2009), p. 85-86.

Activity 2 : what's so special about cyberbullying ?

Related app questions: questions 1, 6, 14, 15 and 23 from the “test your knowledge” quiz and questions 2-9 and 11 from the “how about you?” quiz.

Timing: 20 minutes.

Age group: 10-18 year olds.

Homework: none.

Pre-requisites: activity 1.

Related activities: activity 3, 4 and 6.

Objectives: to identify the differences between bullying and cyberbullying, to realize why cyberbullying is such a big deal.

Online homework and lesson:

Prepare a short online quiz for your students using Google forms or any other online quiz making tool with the following 5 questions (agree/disagree):

- Bullying is worse than cyberbullying because you can actually get physically hurt/injured.
- Cyberbullying is worse than bullying because it can spread much faster to a much wider audience.
- Bullying is worse than cyberbullying because it can lead to getting valuable items stolen such as your wallet, phone, watch...
- Cyberbullying is worse than bullying because it can go on 24/7 even while you're at home where you are supposed to feel safe.
- Cyberbullying and bullying are totally independent from each other.

For each of these questions, make sure that students write down their reason for agreeing/disagreeing with each of these statements.

During the lesson, project the result of the quiz and discuss each of the questions with the students. (15 minutes)

At the end of the lesson, draw on the elements below to underline the core differences between bullying and cyberbullying. (5 minutes)

Offline lesson:

Ask the students to work in groups of three or four and decide either to formulate three arguments defending one of two ideas: that bullying is worse than cyberbullying or that cyberbullying is worse than bullying. (3 minutes)

Ask for volunteers or pick two groups defending opposing ideas if possible and have them present their arguments and debate. At the end of the debate, ask students to vote for the most convincing idea. If all groups chose to defend the same idea, have two groups present

and ask students to vote for the group that presented the most convincing and comprehensive presentation. (10 minutes)

Summarize the ideas stemming from the debate and present some of the following core differences between bullying and cyberbullying. (5 minutes)

What's so different about cyberbullying? Why is it such a big deal? Why could it be deemed worse than bullying?

Can cyberbullying be more harmful than bullying in the physical world?

- Cyberbullying can happen **24/7 at any time, any day and especially any place** (at the victim's home for instance, removing any feeling of safety and security even in his/her own house).
- The **potential audience** for circulating humiliating or hurtful images, texts, videos... **is huge** and the **dissemination is virtually instantaneous**.
- **Deleting the hurtful material can be difficult** if not impossible. Online service providers such as social networks or blogs have a relatively poor record of permanently taking down cyberbullying material in a timely fashion (as opposed to copyright infringement material) and the original copy of the material can be posted across other platforms or reposted if deleted again.
- The cyberbully has the feeling that he/she can remain **anonymous** and although it is possible, it can be very **hard to clearly identify the perpetrator(s)** without reasonable doubt. Sometimes, the cyberbully doesn't even know the victim and vice versa!
- Cyberbullying can be harsher due to the fact that **the bully cannot see the immediate reaction of the victim and experience empathy, guilt or be convinced that he/she has taken it too far**. The victim can also suffer greatly by not knowing exactly how many people including classmates have seen a hurtful text message, picture or video and what their reaction was. This often translates into refusing to attend school.
- **Many measures taken by adults can make things worse** as they are counter-intuitive to situations of traditional bullying. For instance, taking away access to the internet (confiscating a computer, smartphone...) or deleting hurtful messages or material makes things worse. Cyberbullying doesn't stop just because the victim has no access to the internet or because some material or messages were deleted, it only aggravates the powerless feeling of the victim who is left to imagine the dreadful things being shared online and makes it more difficult to investigate cyberbullying and identify the perpetrator(s).
- The **"signs" of cyberbullying are harder to identify** as opposed to bullying, making it more difficult for the people surrounding a victim to identify cyberbullying and help him/her. While in many cases bullying leaves physical traces and evidence that is relatively easy to spot (a broken or stolen good, a trace of a physical aggression...), cyberbullying is only evident by taking away the electronic device of the victim and exploring his/her accounts, messages, etc. thereby also violating his/her right to privacy.

Note: The differences between cyberbullying and bullying described above do not mean that bullying is not a serious issue. They are only meant to underline some core differences between the two. Ultimately, each individual will be affected in his/her own way by face-to-face bullying or cyberbullying.

Activity 3 : consequences of cyberbullying

Related app questions: questions 3, 6, 7 and 10 from the “test your knowledge” quiz.

Timing: 25 minutes.

Age group: 10-18 year olds.

Homework: none.

Pre-requisites: activity 1.

Related activities: activity 2 and 4.

Objectives: to learn about the seriousness of cyberbullying and the related legal consequences

Ask the students to group in pairs of two. One student will be playing the role of the perpetrator of cyberbullying and the other the role of the victim. Ask them to come up with at least 5 situations/actions of cyberbullying with the perpetrator reading out his cyberbullying action, the consequences of these actions (possible legal implications...) and the victim enacting his/her response and how it would have affected him/her. In case students need extra inspiration, you can help them by creating a list of situations based on Annexe 1 (the list of questions from the “have you experienced” section). (5 minutes)

Call for volunteers or handpick a pair of students to act out in a “forum theatre”³ style the different situations. After each situation is being enacted ask the audience (the rest of the students) to comment on two aspects: what could be the consequences for these actions for the perpetrator and how they could affect the victim. (12 minutes)

Distribute the newspaper article provided in Annexe 2 and have students read it (3 minutes).

Spend the rest of the time in discussing the content of the article with students and complementing their findings regarding the consequences of cyberbullying for the victim and the perpetrator(s) with the elements below. (5 minutes)

For the **victim**, studies point to many serious consequences:

- **negative emotional responses** such as fear, anger, sadness, frustration, powerlessness, lower self-esteem and confidence, depression;
- **negative behavioural responses** such as isolating oneself, lack of concentration, lower school results, missing school, being pressured into delinquency, revenge and retaliation against the cyberbully or someone else,
- **extreme responses** such as self-harm, attempts of suicide or suicide.

These consequences are intrinsically linked to the specific nature of cyberbullying as discussed in activity 2 (cyberbullying can go on 24/7, the victim can feel powerless about it... see above).

Besides laws covering **harassment** in national laws, the **Data Protection Directive** (95/46/EC) that applies to all European Member states can also be used as a legal basis to address cyberbullying. Data protection plays a role because “whenever personal data of

³ http://en.wikipedia.org/wiki/Forum_theatre

individuals is collected by electronic means; for example, in Internet forums, in social networks, by using instant messaging or email communication, [t]he legislation sets forth various principles that must be respected by those [...] who publish information about third parties."⁴

What this means is that whenever a cyberbully discloses personal information about a victim, the provisions of the EU Data protection directive are fully applicable, since sharing such information requires the consent of the individual beforehand. The responsibility lies therefore in the hands of the cyberbully who, by processing and disclosing personal data, becomes a "data controller" and as such, has serious legal responsibilities associated to this role. The 2003 ruling of the ECJ (European Court of Justice) on the Lindqvist case⁵ confirms this interpretation.

Victims can, on the basis of this law, launch a complaint about the violation of their data protection rights to the supervisory data protection authorities or in a court.

Activity 4 : what should you do in case of cyberbullying?

Related app questions: questions 4 and 5 from the "test your knowledge" quiz.

Timing: 30 minutes.

Age group: 10-18 year olds.

Homework: none.

Pre-requisites: activity 1.

Related activities: activity 2 and 3.

Objectives: to acquire some basic knowledge about how to react in case of cyberbullying as a victim or a bystander (witness).

Ask students to work in groups of three or four and instruct them to create a short 5 minutes enactment of how they would react in three different situations of cyberbullying, with one student being the victim and the others being bystanders (witnesses). In case students need extra inspiration, you can help them by creating a list of situations based on Annexe 1 (the list of questions from the "have you experienced" section). (5 minutes)

Ask for volunteers or pick two groups and have them present how they would react in the three situations of cyberbullying they have come up with. Allow some time between each enactment for comments from the rest of the class (15 minutes).

Based on the two presentations, ask the students to identify key tips for bystanders and victims of cyberbullying. (5 minutes)

⁴ Giovanni Buttarelli, "Data protection legislation in Europe, preventing cyber-harassment by protecting personal data and privacy", 07/06/2010,

http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-06-07_Speech_Cyber-harassment_EN.pdf

⁵ <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01>

Show students the #DeleteCyberbullying awareness video on YouTube. (3 minutes)

<https://www.youtube.com/watch?v=dkG00Czb4ho&list=UUSfCFQyV7annlf60sjxGGTQ>

Compliment the tips students identified with some of the following core tips to address cyberbullying both for victims and bystanders. (2 minutes)

The most common tips for victims of cyberbullying are the following:

- **Do not respond** to cyberbullying messages and **do not forward** them, and especially, **do not cyberbully back** (this usually makes things worse);
- **Save the evidence** of the cyberbullying (print screen, save on hard drive, record the dates and times of the cyberbullying actions,... all of these are needed to prove that cyberbullying took place in case there is a formal investigation);
- **Block the bully, let him/her know that you are hurt by his/her actions and ask him/her to stop** (although this might not have any effect on the cyberbully or cyberbullies, it is also a standard procedure: it has to be done in order to take the problem forward with the school authorities or even law enforcement);
- **Report the incident to the administrator of the website** (social networking sites and video sharing sites should have a way to report cyberbullying: even if they are not always 100% effective, it is a standard procedure that needs to be carried out);
- **Talk to an adult you can trust** (your parents, your school teacher, or any other adult) **or a trusted friend**;
- **Get in touch with a helpline** in your national country if you have specific problems you want to discuss (see the #DeleteCyberbullying app to get in touch with a helpline);
- **Contact the police** with the help/assistance of a trusted adult if the cyberbullying hasn't stopped.

Bystanders can be peers but also any other person who witnesses cyberbullying while it happens (a perpetrator(s) sending or posting something or a victim receiving something).

Although bystanders are usually passive and are not willing to get involved for fear of bringing cyberbullying (or bullying) on to them, their role is crucial in the early detection of cyberbullying and intervention. What they can do is akin to what was seen above:

- take note/save what they have witnessed as evidence to prove the cyberbullying;
- step up for the victim and make it clear that they do not approve of the cyberbully's behaviour;
- talk to a trusted adult about what they have witnessed;
- never encourage or indirectly contribute to the cyberbullying (forwarding a message, "liking" inappropriate or hurtful jokes...)

Activity 5 : privacy online, why bother ?

Related app questions: questions 9, 11, 17-21 and 23 from the “test your knowledge” quiz and questions 3, 4 and 7 from the “how about you” quiz.

Timing: 35 minutes.

Age group: 14-18 year olds.

Homework: before the lesson, ask students to research any news relating to privacy issues online.

Pre-requisites: none.

Related activities: activity 6 and 7.

Objectives: to understand the implications of over-sharing online and the importance of thinking before you post.

Prior to the lesson, ask students to research stories in the news about online privacy breaches in the last few months and respond to a series of questions:

- Have you heard about such a story before?
- What would you have done in a similar situation?
- How do you think the concept of privacy has changed with technologies such as the internet?
- Do you believe we should mostly change our behaviours or do social norms need to change and evolve too?

During the lesson, ask for volunteers or pick students and have them present their thoughts and make them debate about the two last questions. Encourage students from the class to engage in the debate. For the fourth question, especially, you may stage a parliamentary style debate. Split the room in two halves with on one side, students wishing to defend the opinion that we should mostly change our behaviours online and our use of new technologies (social norms should stay the same but we should learn to use new technologies and the internet more wisely) and on the other side, students wishing to defend the opinion that our social norms need to change to adapt to new technologies and the internet (some concepts such as privacy cannot remain the same). Try to have roughly the same amount of students on each side of the debate and take up the role of the moderator. (20 minutes)

Optionally, you can distribute the articles in Annexe 3 and shortly analyse them with students, showing that online privacy breaches can have a very wide range of consequences from losing one’s job to being robbed etc. (5 minutes)

At the end of the debate, you may distribute Annexe 4, which is a document of 10 tips to protect your privacy online prepared by the European Parliament. Have the students read them and briefly share their thoughts about them. (10 minutes)

Activity 6 : how does the internet work ?

Related app questions: questions 13, 14, 15, 22 and 28 from the “test your knowledge” quiz.

Timing: 40 minutes.

Age group: 12-18 year olds.

Homework: after the lesson, ask students to find out about “hops” and accessing online material.

Pre-requisites: none.

Related activities: activity 5 and 7.

Objectives: to understand the basic functioning of the internet and some of the implications.

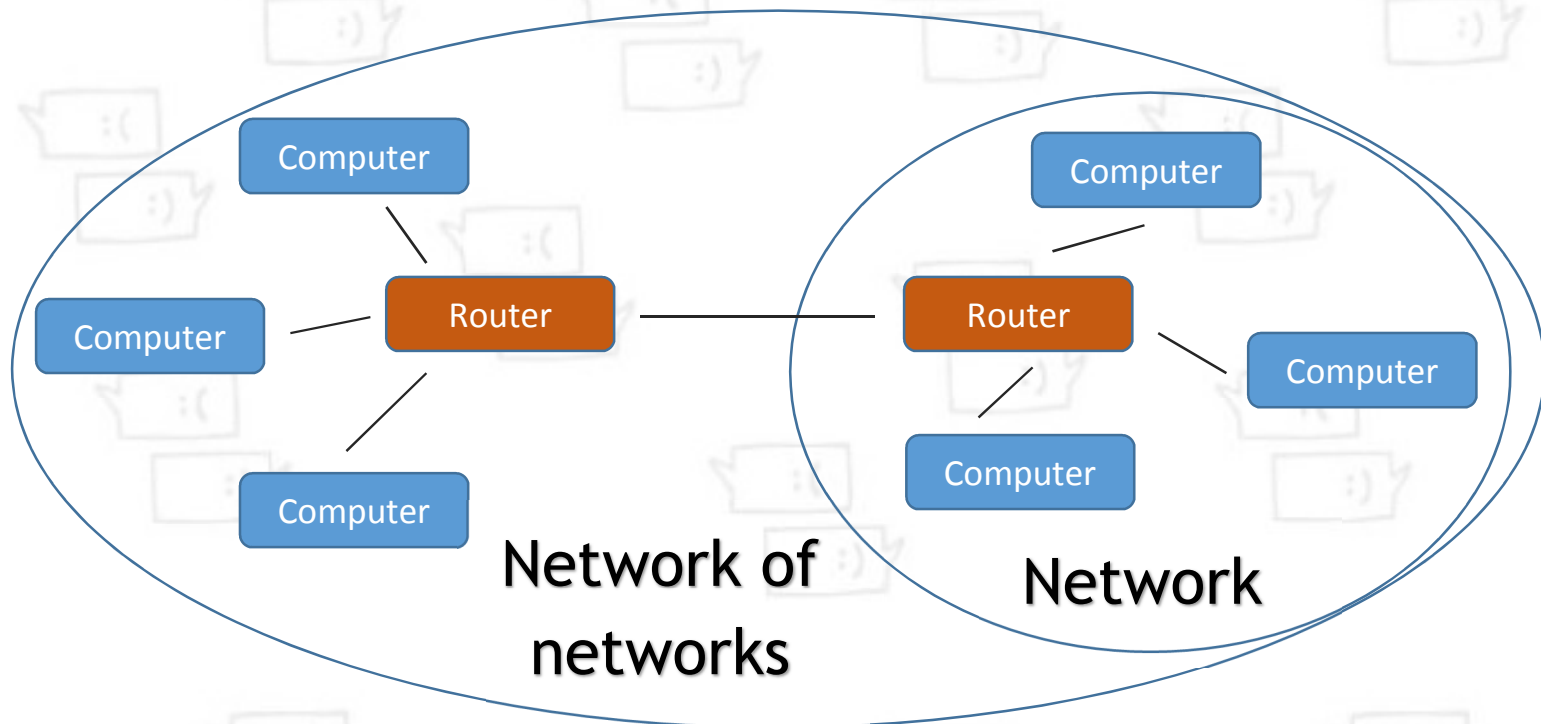
Ask the students to work in groups of 3 or 4 and write down a diagram of the internet starting from their computer and answer these questions (5 minutes):

- Where is the data that you share online stored? (Pictures on social networks, articles on blogs, videos on streaming platforms...).
- What do these terms and acronyms mean: hop, IP, packet, router, ISP and data server.

Call for volunteers or handpick a group to draw their diagram on the board and share the definitions they came up with. Ask the other groups to complement/comment on the diagram and definitions. (5 minutes)

Distribute Annexe 5, explain the diagram and definitions according to the elements below (20 minutes).

When two or more computers are connected together, they form a network. The larger the network gets, the more complex the “rules” are for ensuring that they can communicate to each other (transmit information). The internet is a “network of networks” which essentially means that a set of computers forming a network are connected to other sets of computers forming a network.



Definitions:

A **hop** (in networking) is part of the path that data takes between its origin and its destination (for example, a “hop” is the path between a users’ computer and the ISPs router, or between the ISPs router and a “backbone” router of the internet). To access a Japanese website for instance, the request from the user to display the website and the data transmitted back to the user involves a large number of “hops”, each taking only a few milliseconds.

- An **IP** stands for “**I**nternet **P**rotocol”. It is the communication protocol enabling the delivery of a packet from the source host to the destination. For instance, one of the IP addresses of Google is 74.125.224.72. If you type these four numbers into your web browser, it will display the Google search engine website. But since IP addresses are not very “practical” to memorise, humans use URLs (Uniform resource locator) or web addresses instead that correspond to an IP address.
- A **packet** is a formatted unit of data. In order to transmit data across the internet from a website to a user or between two users, data (picture, video, document, website) is broken down into smaller parts called “packets”. Packets carry **control information** and **user data**. Control information contains information that helps the network deliver the data transmitted from one point to the other at each “**hop**” (such as address of the source, address of the destination, error detection codes and information on how to assemble that packet with other packets to reconstitute the data once the transmission is completed). The user data is a small part of the actual data being sent or received.
- A **router** is a network device (a piece of specialised hardware) that forwards **data packets** between computer networks. These are key in making sure that your data finds its way to its destination. The device that connects multiple computers between each other in your home is also called a router because it forwards your data packets between them. Very often, it also acts as a “modem”, connecting you to your ISP to gain access to the internet. Your ISP, in turn, forwards your data packets via much more sophisticated routers and so on until the data reaches its intended destination.

- An **ISP** stands for an **Internet Service Provider**. It is an organisation or a company that provides the service that allows you to access, use or participate in the internet. It is basically the “gateway” for users to entering the backbone of the internet.
- A **data center** is a facility that hosts a large number of computers for various purposes such as telecommunications or data storage. This is also where much of the internet’s data (websites, files...) is stored. Some large companies such as Google, Microsoft or Facebook have their own data centers⁶.

A simplified version of the internet is comprised of different “levels” (see the first illustration of Annexe 5). The first level is that of the **users**, individuals such as students and their families that have devices that connect to the internet via a landline connection (phone line, cable TV...) or a wireless connection (mobile data...). These users connect to an **ISP** (internet service provider) which provides the “gateway” to the “backbone” of the internet (key, strategic points that allow networks to be connected between themselves). Many of these can be seen in the **underwater cables illustration** in Annexe 5. Most of the data that transits across continents goes through underwater cables and at each end of these cables, there are large facilities filled with routers and other pieces of hardware that makes sure that the data sent or requested by users arrives at the intended destination. Originally, all data used to travel via physical cables but nowadays, data can also be sent via wireless networks such as mobile devices. Data sent from a mobile device travels to the mobile operators’ “towers” or “base stations” and is then redirected to the internet. Information can also transit via satellites.

In order to work, the internet relies on a number of complex rules. One of these is the **Internet Protocol (IP)** that provides a unique number to each machine connected to the network (similar to the postal address of a house) in order for data sent or requested to find its way. Data transmitted is also broken down into smaller fragments called “**packets**” for a more efficient communication. Instead of sending one large file in an uninterrupted signal, the data is sent in smaller parts via short signal “bursts”. This allows for mostly two things: virtually simultaneous receipt and sending of various data (you can download a file while streaming a video) and increasing the success of the communication (should a packet fail to reach its destination, the destination’s computer can send a request for that specific packet to be resent instead of having to resend the whole piece of data).

What are the implications? Why is it important to know how the internet works?

Ask the students to reflect on these two questions (2 minutes) and call for volunteers or hand pick several students to present their reflections (3 minutes).

Present some of the elements below (5 minutes):

- Since the internet is decentralised and no country fully controls it, the information or data (text, pictures, videos, documents...) that you send online can escape your own control. The saying “**what goes online stays online**” carries much truth especially in the case of a tier (an external person) gaining access to that piece of data and reposting it elsewhere. The data that you send is in most cases hosted in a foreign country and having your data removed can be a very difficult if not impossible task. In the EU, the revised Data Protection Directive now gives you the “right to be forgotten” by sending a request to search engines to remove your name from search queries. But this does not mean that the data is deleted, it only means that it cannot be found via a search engine such as Google or Bing.

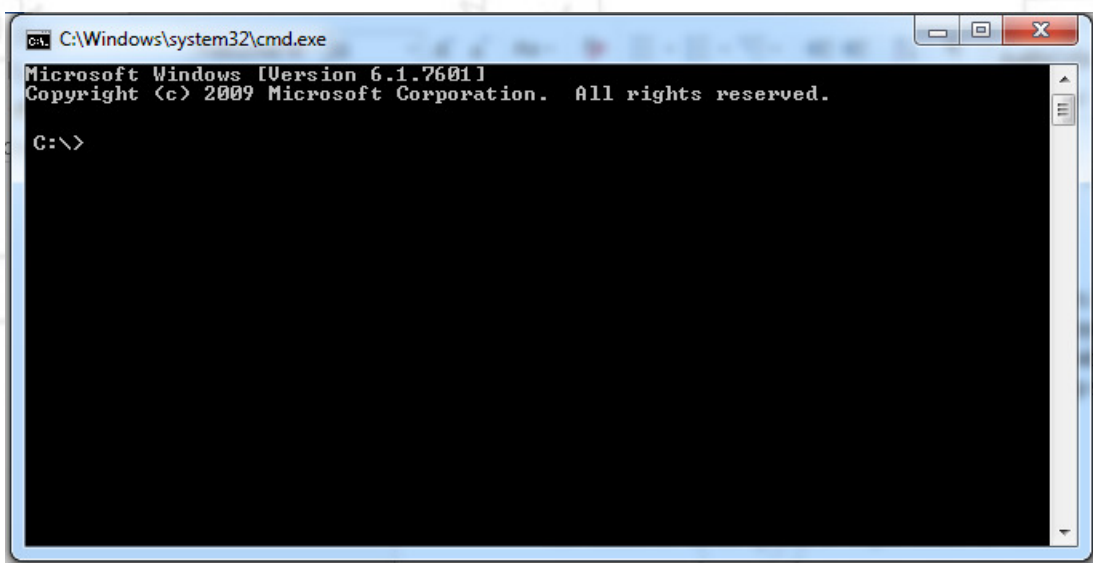
⁶ <http://www.google.com/about/datacenters/inside/locations/index.html>

- When requesting data or sending data over the internet, the data transits through a certain number of points. At each point, there is the **possibility of a security breach and your data being compromised** (spied, lost, stolen, etc). The recent revelations from **Edward Snowden** showed that states can spy on the internet by controlling key points in the network such as the land based stations that process the communication from underwater cables. Vulnerabilities also exist in the wireless connection between mobile devices and WiFi routers. For instance, if you connect to a “public wifi” network (in an airport, train station,...) and do not make sure that your connection is secured, the data that is being send or received could be “sniffed” or “analysed” by someone else connected to the same WiFi router. Viruses and malware can also compromise your very device, enabling access to your data remotely when your device is online. Finally a large number of applications are now connected to the internet 24/7 on mobile devices: facebook, whatsapp, skype, email clients, google now,... all of which are “listening” to any data that is destined to them such as a message or notification. These permanent connections can also contain vulnerabilities that can be exploited to compromise your device and data. This is why it is so important to always update your software.
- The way the internet was designed also means that **no one can be 100% sure to remain anonymous**. Law enforcement, with the proper legal backup (mandate from a court), can investigate and identify users breaking the law online. This includes authors of cyberbullying, users violating copyright and so forth. There are many ways to find out who is behind an online post. Websites keep track of the IPs of individuals that interact with a website. ISPs also keep some record of the data transmitted via your internet connection.

Bonus activity for students to try at home:

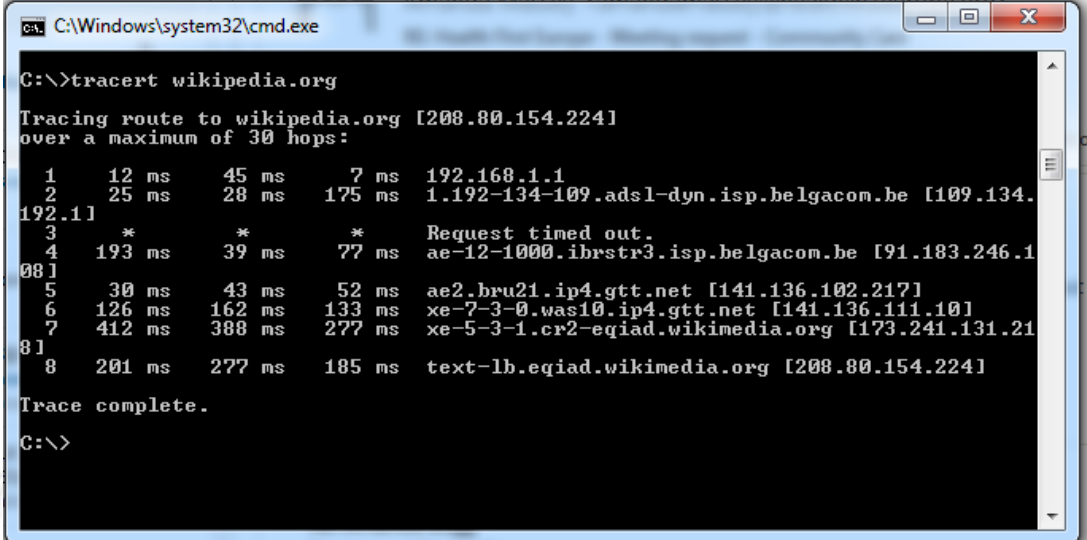
On Windows 7 and above:

- 1) Click on the “Start” button in Windows.
- 2) Type “cmd” in the “search” bar and click on the program icon that shows up in the start menu.



- 3) Type “tracert wikipedia.org” and press “enter”.

- 4) You will then be able to see the “hops” that exist between your computer and the website you are trying to reach and how much time each “hop” takes. In this example, we see that to access Wikipedia, we first go through routers of our “local” ISP (in this case Belgacom from Belgium), then goes across the Atlantic to a router in Washington (abbreviated “was”), finally to arrive to the place where Wikipedia is hosted. Students are of course encouraged to try this with other websites.



```
C:\Windows\system32\cmd.exe
C:\>tracert wikipedia.org

Tracing route to wikipedia.org [208.80.154.224]
over a maximum of 30 hops:

  0  12 ms  45 ms  7 ms  192.168.1.1
  1  25 ms  28 ms  175 ms  1.192-134-109.ads1-dyn.isp.belgacom.be [109.134.192.11]
  2  *      *      *      Request timed out.
  3  193 ms  39 ms  77 ms  ae-12-1000.ibrstr3.isp.belgacom.be [91.183.246.108]
  4  *      *      *      Request timed out.
  5  30 ms  43 ms  52 ms  ae2.bru21.ip4.gtt.net [141.136.102.217]
  6  126 ms  162 ms  133 ms  xe-7-3-0.was10.ip4.gtt.net [141.136.111.10]
  7  412 ms  388 ms  277 ms  xe-5-3-1.cr2-eqiad.wikimedia.org [173.241.131.218]
  8  201 ms  277 ms  185 ms  text-lb.eqiad.wikimedia.org [208.80.154.224]

Trace complete.
C:\>
```

On Mac OS X and above:

- 1) Launch the network utility in Mac OS X (you can do this by going into Spotlight and typing “Network Utility” and clicking on the top hit).
- 2) Click on “Traceroute”.
- 3) Enter the domain name for which you want to perform a traceroute like “Wikipedia.org” and click on Trace.
- 4) You will then be able to see the “hops” that exist between your computer and the website you are trying to reach and how much time each “hop” takes.

Optional material for the teacher: <https://www.youtube.com/watch?v=oj7A2YDgIWE>

Activity 7 : the internet of spam, scam and advertising

Related app questions: questions 9, 16, 24, 25 and 30 from the “test your knowledge” quiz.

Timing: 50 minutes.

Age group: 14-18 year olds.

Homework: before the lesson, ask students to do some research on the business model of the services they use most online (how the services they use make money). See below for details.

Pre-requisites: none.

Related activities: activity 5 and 6.

Objectives: to understand the commercial incentives behind the internet and how it impacts the users’ experiences online.

Homework assignment:

In preparation for the lesson, ask students to pair in groups of three or four to carry out some research at home. Students are encouraged to use online collaborative platforms such as Dropbox, Google Drive, One Drive etc. Each group will present the business model of one of the following online services/games/content providers:

- Wikipedia
- Facebook
- Google
- Netflix
- World of Warcraft
- League of Legends
- Instagram/Whatsapp

Optional if all of the above are assigned to a group:

- Amazon
- Youtube

Their research should answer the following questions:

- What is the main source of revenue (the business model) for these services?
- What are the various payment systems other than cash (credit card, debit card...)?
- How, according to you, could business models and payment methods affect the end product/service/content and your experience as a user?
 - o *For instance, if a website relies on advertising, then it affects the website’s design since it needs to think about including advertising spaces. This also means that it may affect the readability or appeal of the website for users such as yourself.*

Lesson:

On the day of the lesson, ask all groups to step up and present their findings for the first questions above (2 minutes for each group, between 10 to 15 minutes total).

In case students didn't cover these aspects, supplement the students' presentations (the advantages and disadvantages will be useful in the next activity):

- Wikipedia: The business model relies on donations.
 - o Advantages: relies on people's better nature, independent from private interests, not overwhelmed by advertising.
 - o Disadvantages: cannot guarantee a steady revenue stream and long term financial viability, may need to resort to "advertising" for obtaining donations which may end up being just as intrusive as regular advertising.
- Facebook: The business model relies on advertising for the most part and payment from Facebook games/apps etc.
 - o Advantages: ensures a growing revenue stream (based on the current trends), users do not need to pay a subscription to use the service (they pay with their private data and the time they spend looking at/interacting with/clicking on advertisements).
 - o Disadvantages: dependent on the enduring and massive user base and therefore has to aggressively tackle competition such as other social networks (if people stop using Facebook, the revenue from advertising would collapse), raises concerns over privacy and data protection, subject to pressure from private interests, balancing user generated content and advertising may be difficult (too much advertising might set people off, too little might damage revenue), runs the risk of overly manipulating social interactions between people (manipulate the newsfeed) to optimize revenue rather than ensure neutrality and visibility of people's news, engaged in a permanent effort to ensure that users stay as long as possible on Facebook since the longer they stay, the more revenue Facebook can pull from advertising (there is a vested interest in ensuring people spend/waste as much time as possible on Facebook. This is also true for users' participation: the more data users share on Facebook the better they can be targeted with ads.)
- Google: The business model relies mostly on advertising with some revenue from sales of products/services (such as consumer products like Google smartphones or the upcoming Google Glass, internet service provision, etc.)
 - o Advantages: ensures a growing revenue stream (based on the current trends), users do not need to pay a subscription to use the service (they pay with their private data and the time they spend looking at/interacting with/clicking on advertisements).
 - o Disadvantages: dependent on the enduring and massive user base and therefore has to aggressively tackle competition such as other search engines, email providers or social networks (if people stop using Google products and services, the revenue from advertising would collapse), raises concerns over privacy and data protection, subject to pressure from private interests, balancing user generated content and advertising may be difficult (too much advertising might set people off, too little might damage revenue), runs the risk of overly manipulating search results or newsfeeds to optimize revenue rather than ensure neutrality of content displayed in the search engine as well as on its social network, engaged in a permanent effort to ensure that users stay as long as possible on Google's services since the longer they stay, the

more revenue Google can pull from advertising (Google has already been accused of closely integrating all Google services such as the search engine, Google Maps, Youtube, Gmail etc to Google+ to pressure users to subscribe to G+ and spend more time on it. The same goes for users' participation: the more users search for things via Google, send emails via Gmail or share data on Google+, the better they can be targeted with ads).

- **Netflix:** The business model relies on monthly user subscription fee.
 - o **Advantages:** easy for users to understand, ensures a steady and predictable revenue stream, no advertising or abuse of private data.
 - o **Disadvantages:** users pay the same amount regardless of the intensity of their use which may “pressure” them to “maximize” what they pay for (some users may feel “obliged” to use the service just to get their money’s worth), other competing business models such as “freemium” or “free with advertising” might drain the user-base.
- **World of Warcraft:** The business model relies on monthly user subscription fee.
 - o **Advantages:** easy for users to understand, ensures a steady and predictable revenue stream, no advertising or abuse of private data (although this greatly depends on the game: since World of Warcraft is staged in a “fantasy” world, it is much harder to integrate advertising. There have been other online games that take place in a “real world” setting where ads were included in the game as part of the décor).
 - o **Disadvantages:** users pay the same amount regardless of the intensity of their use which may “pressure” them to “maximize” what they pay for (some users may feel “obliged” to use the service just to get their money’s worth), other competing business models such as “free-to-play” or “free with advertising” might drain the user-base.
- **League of Legends:** The business model relies on a “free-to-play” or “freemium” business model. It is free to play the game but to get access to some additional content or to make progress much faster, you need to pay.
 - o **Advantages:** users pay proportionally to their needs (heavy users will pay more than light users), users can test the game/service/content freely before they need to pay anything.
 - o **Disadvantages:** risk of stagnation since there is no steady revenue there is less incentive to upgrade the content/game/service, the balance between what is freely accessible and what is to be paid for is very difficult to find (if too many things are for free there is no incentive to buy anything which lead to having no revenue, if too many things need to be paid for users might be discouraged from playing/using the service/accessing the content altogether).
- **Instagram/Whatsapp:** This is not exactly a “business” model but rather a “strategy” called “build to sell”. This relies on giving a software/service/content for free, building up the user base, and hoping to either find a business model along the way (like including advertising once you have a huge user base like Snapchat has recently considered doing) or sell to a huge company once you have reached a certain popularity and have a huge number of users.
 - o **Advantages:** there is no need to worry about money at the start of the “project” so it takes less time to make it available to users, the software/service/content can be used for free by users.
 - o **Disadvantages:** there is no guarantee that the software/service/content will be able to “survive” financially and it may disappear after some time, after

finding a business model for instance by selling to a huge company (both Instagram and Whatsapp were bought by Facebook) the software/service/content can change substantially and alienate the existing users (for instance with excessive advertising, a change in the design or functionality, having to suddenly pay for it...)

- Amazon: The business model is the same as any big retailer such as Carrefour, Tesco or others. It's a fixed cost business which uses the internet to get the maximum out of its fixed assets (warehouses and shipping centres...): by selling high enough volumes of goods, it can exceed its fixed costs and thus create a profit.
- Youtube: The business model relies on advertising (pre-screening video ads).

General note: There is no single business model that can guarantee that all information and content on the website or service is of high quality and is credible. The credibility of online content can only be measured by the internal policy and identity/ownership of the website (peer reviewed content, extensive use of citations, owned by a reputable academic institution etc) rather than by the underlying business model.

Online and other digital payment methods:

- Online money transfer services such as PayPal.
- Virtual online accounts such as Google Wallet, Amazon Payments,...
- Global virtual currencies such as Bitcoins or local virtual currencies such as those found in online games like League of Legends.
- Credit cards (such as MasterCard, Visa... with or without a security token).
- Debit cards (via e-banking and a security token)
- NFC (Near Field Communication): this technology allows contactless payment with smartphones or credit cards equipped with NFC simply by approaching the device or card to a receiver.
- Mobile payment: this includes all the various ways via which one can pay using his/her mobile such as premium SMS services, direct operator billings (expense added to your mobile operator bill), online wallets etc.
- Data: interestingly enough, a "new" form of currency online is information about users which allows to customize advertising to them.

Ask the class which business models, according to them, are the most common and the most popular (5 minutes debate).

Distribute Annexe 6, ask the students to examine it and identify some key trends. Ask for a group to share their findings (5 minutes).

If students didn't underline the following trends, make sure you point them out:

- Advertising revenue for most online internet services is rising which also means that advertising expenditure (how much companies spend on advertising online) is also rising.
- An increasingly popular and widespread business model is the "freemium" one.

Ask the students why the "freemium", "free-to-play" and advertisement driven business models are the most successful and write down the feedback on the blackboard, complimenting their answers with the elements above (advantages and disadvantages) and below (summary of the reasons). (5 minutes)

- The “freemium” or “free-to-play” model’s success stems from the following benefits for users:
 - o it’s “free” to use it up to a certain level,
 - o users can test it before having to pay anything,
 - o heavy users will pay for premium services and light users can stick to the “free” version,
 - o users can upgrade and pay for features at any time.
- The advertisement model’s success stems from the fact that users perceive that it is “free” to use and have a low level of understanding about the “price” they pay for the software/service/content (exploitation of their private data to better target them with advertisings).

Ask students to reflect on how these two business models affect the software/services/content they are using/accessing (drawing on their findings from their homework) and complement their contributions with the elements below (10 minutes).

- The “freemium” or “free-to-play” model may have the following influence:
 - o The software/service/content you are using/accessing will be designed to induce addictiveness and exploit it to ensure users invest money in premium features. For instance, at key moments in a game, the user will be obliged to pay for premium content to advance.
- The “advertisement” model may have the following influence:
 - o An attempt to maximize the time you spend on their software/service/content to increase ad revenue. It implies trying to capture users’ attention and making sure they stay for instance on a given website as long as possible. The impact on the user means that entire websites are desperately trying to waste the users’ time in order to maximize their advertisement profit. This term is called “stickiness” in the online advertising jargon.
 - o With the dawn of targeted advertising, online services such as social networks have a vested interest in making sure people share as much information about their lives as possible. Advertisers buying ads on a social network rely on the premise that their money is invested much more efficiently than real life ads since they can precisely determine who sees this ad, filtering by age, sex, location, language/country, level of education and whatever other information you may have shared (the music/movies you like, your hobbies etc).
 - o The presence of private companies on social networks and other services relying on advertising for revenue means that any user can become a marketing agent for the private company. For instance, if you like a brand on Facebook, this gives that company the right to display advertising to your friends saying you like their company/product. On Youtube for instance, users can now make money by including a pre-screening video ad before their video, which also transforms the creators of Youtube videos into advertisers. It creates a strong incentive to maximize your viewership and going viral at any cost (at the expense of the underlying quality of the content for instance, posting humorous/silly content rather than educational content). Even more disturbing, users that post videos or blog posts online and gain a large viewership are approached by companies to directly plug products or brands into their content.
 - o To sum up, the most successful advertisement campaigns are the ones that secure users’ engagement by interacting, commenting, liking, sharing... an ad or a product. An example of such a strategy is the Coca-Cola “Share a coke” campaign, where users themselves engaged in posting pictures of

Coca-Cola bottles with their names or their friends' name on it, thereby serving as a multiplier for the campaign with no additional cost for Coca-Cola. (see Annexe 7 for examples)

Ask students to reflect on how the growing number of new payment methods affect their online environment especially regarding spam and scam and complement their contributions with the elements below (10 minutes).

- With the growing number of new payment methods, there are that many more ways to “extract” money from internet users, be it via legal or illegal ways. This also includes extracting data and information from users (such as social networking profiles, posts, content of emails, web search keywords, even geolocation data).
 - o *Advertising*: on the “legal” side, as it was shown in the trends exposed earlier (growing e-commerce and growing investment in online advertising), there is a strong incentive to advertise to users given that it is easier than ever to purchase things online.
 - o *Spam*: on the border between “legal” and “illegal”, we find a great deal of spam which can either be overly intrusive advertising or simply scam. The term was mostly used for unsolicited emails polluting ones email account but can now extend to much more such as posts or invitations on social networks, comments on videos, comments on blogs, etc.
 - o *Scam*: on the “illegal” side, we find attempts at tricking the user into spending money or compromising his data (social network account, email account...). This has also grown tremendously over the years as online payment has become easier. (An example of this can be found in Annexe 7, where the user has to enter his/her phone number to win an iPad, which results in being subscribed to a premium SMS service that drains money from their mobile card)
- In conclusion, facilitated online payment methods and new valuable currencies such as user data has encouraged the growth of advertising, spam and scam. The online environment users experience is filled with all three and significant efforts are made to ensure users cannot tell the difference between ads, spam and scam. For instance, attempts at stealing ones' password to email or social network accounts (phishing) have become more difficult to spot: emails received by the user look like “genuine” emails from their email provider or social network. A lot is also being done to mislead users into clicking on an ad/spam/scam instead of the content they originally seek by “blending” ads/spam/scam into the content seamlessly (for instance by creating big “download” buttons that redirect them to another content and a smaller less obvious one for downloading the actual file they are seeking).

How is this linked to cyberbullying?

Cyberbullying is mostly a matter of behaviour and people, but it is enabled by technology. Cyberbullying is happening on many online platforms, services, websites, games, devices... and the way they are configured, their internal policies, default settings, privacy protection features and business models can sometimes exacerbate or make cyberbullying someone “easier”.

For instance, many services including social networks rely on a variety of elements to generate revenue from advertising. Among these, we find **maximizing user participation** (sharing, commenting, posting, interacting, liking etc) since this will enable them to sell more detailed information about their users to advertisers and thereby maximize the impact of their advertising campaigns, targeting very precisely specific users based on the massive amount of data and information they generate. This also means that these services have an interest in ensuring that **people keep their profiles open** (as opposed to completely locking down your account which would mean that your posts/actions will be seen by a restricted audience) and **keeping as much data about users as possible** (thereby discouraging users from “cleaning” their accounts regularly or deleting a vast amount of long past contributions/posts...)

One can easily see that these factors can enhance the likelihood of someone being cyberbullied or make it harder to block it (open profile, low control over one’s data...)

This is but one example of how a specific business model influences the outcome of human behaviour.

ANNEXE 1: FULL LIST OF APP QUESTIONS

Questions in the “Test your knowledge” section (correct answers in bold)

1) What is cyberbullying?

- Sending a one off insulting message to someone.
- Forcefully taking a mobile phone away from someone and deleting all his/her data before giving it back.
- **Trying to hurt someone intentionally by sending him/her repeated insulting messages or pictures online.**
- Sending emails to all your contacts trying to trick them into sending you money.
- Being approached by an adult with bad intentions who forces you to do things you don't want to do online.

2) How many of your classmates have experienced cyberbullying?

- Less than one in twenty.
- Less than one in ten.
- **About one in five.**
- One in two (50%).

3) A friend of yours is being cyberbullied. How serious do you think it can get?

- Nothing serious. My friend can easily deal with it on his/her own.
- **It can lead to depression or self-harm. My friend could feel powerless against cyberbullying.**
- It can be frustrating for a short time, but my friend can always delete or ignore things that bother him/her.
- It can have lasting effects on my friend's reputation.

4) What should you do if you receive several negative comments/posts or threatening messages?

- Delete the messages and forget about it.
- Respond immediately using the same language.
- **Don't respond, save all the evidence and talk to a trusted adult or a trusted friend.**
- Share it with your friends and contacts to show how bad the message is.

5) If you witness someone receiving continuous harassment messages you should:

- **Help the person being harassed, talk to a trusted adult and if you feel up to it, ask the bully to stop.**
- Do nothing and take your distances as you might be harassed yourself.
- Bully back to let the person know how it feels to be bullied.
- Advise the person harassed to be less of a wimp and avoid provoking bullies.

6) Face to face bullying is much worse than cyberbullying.

- True.
- **False.**

7) What is sexting?

- Sharing pictures of yourself naked.
- Sharing videos of yourself naked.
- Sending texts talking about sex.
- **All of the above.**

8) How can you make sure that a person is who he/she says he/she is online?

- Ask for a copy of his/her ID card.
- Ask him/her to appear on a webcam.
- Ask him/her a secret question that only he/she would know the answer to.
- **You can never be sure.**

9) Why can't you sign up to a social network before you're 13?

- Because social networks are only for adults.
- There are many violent, sexual or shocking things on social networks.
- **A law forbids the use of personal information for commercial purposes below the age of 13.**
- There are minimum requirements for language skills and computer skills to be on social networks.

10) What can be the consequences if you are caught cyberbullying someone?

- Nothing if I remain anonymous and there is no proof.
- Being punished by my parents or by the teacher.
- Being disconnected from the internet by your internet provider.
- **Legal consequences, getting in trouble with the police.**

11) Do you have the right to post pictures that you took of your friends online?

- Yes I can. If I took the pictures, I own them.
- **No, unless I get their permission.**
- I can post the pictures but they can decide to tag or untag themselves.
- Yes, if they were OK with me taking the pictures that means I can share them too.

12) If you like or share a hurtful comment or embarrassing picture of someone, is that also considered as cyberbullying?

- No, someone else posted it.
- **Yes, it can be considered as cyberbullying.**

13) Can you remain anonymous online?

- Yes, if you're good with computers.
- Yes, even if you're not good with computers, just create a fake nickname or profile.
- **No, you can never be certain that you will remain anonymous.**

14) Can you delete pictures or comments once you posted them online?

- Yes, just hit the delete button.
- Yes, unless someone else reposted them.

- Yes, you can ask the online service (Facebook, Youtube) to delete any copies of your post or picture.
- **No, you can never be sure that your posts or pictures are deleted from the internet forever.**

15) Are messages posted on a service that erases them after a set time (for example Snapchat) really gone?

- Yes, that's the way the service is designed.
- **No, there are plenty of ways to override the system.**

16) Which of these methods can you use to identify a phishing attempt? (someone trying to steal the password of one or more of your online accounts)

- The email address from the sender is suspicious (ex: password@1.twitter.com instead of password@twitter.com).
- The content of the email is suspicious (ex: the layout, fonts and images of the email is unusual).
- You are asked to send your account details (username, password...) directly via email.
- The webpage that you are redirected to is suspicious (ex: www.1.twitter.com instead of www.twitter.com).
- **All of the above.**

17) Who is it safe to share your password with?

- My best friend.
- A total stranger.
- My brother or sister.
- My boyfriend/girlfriend.
- **My parents.**
- My teacher.

18) Who is it safe to share your mobile phone number with?

- **My friends and family.**
- My class mates, friends and family.
- Anyone at my school/work, friends and family.
- Anyone who asks to have it, even share it publicly online.

19) What could happen in the worst case if you share your mobile phone number publicly?

- Receiving annoying messages or phone calls from strangers that I have to delete/ignore.
- **Receiving anonymous hurtful messages or phone calls, even being subscribed to services that take money from your phone (SMS services, ringtones...).**
- Nothing, it's safe to share your phone number publicly.
- Receiving advertising messages or phone calls from telemarketers.

20) Who is it safe to share your home address with?

- **My friends and family.**

- My class mates, friends and family.
- Anyone at my school/work, friends and family.
- Anyone, it doesn't matter, it's not sensitive data.

21) What could happen in the worst case if you share your home address publicly?

- Having strangers coming to visit me.
- Receiving annoying mail or advertising in my mailbox.
- **Being harassed by someone or even getting robbed while I and my family are on vacation.**
- Nothing, it's safe to share my home address publicly.

22) Where is all your online data stored? (for instance your vacation photos on social networks)

- Somewhere on the hard drive of your computer.
- **On hard drives of huge warehouses called "data centers" in various foreign countries.**
- On hard drives of the internet service provider in your country.
- On satellites orbiting the earth.

23) Which of these propositions is false? It is important to think before you post online because:

- It may be used to cyberbully you.
- It may prevent you from getting a job if you have posted silly things.
- It may help thieves to gain access to personal information about you that could be valuable to steal from you.
- It will be exploited by advertisers to encourage you to buy more things.
- It might affect negatively how others think about you, or whether others will like you or not. (you might not be popular)
- **It may damage your computer's hard drive.**
- You could end up in trouble with the police if your posts' content is illegal.

24) How do most "free" online services or games make money?

- They are financed by the government (via taxes that are paid by people).
- They get donations.
- **They sell your private information to advertisers and display ads.**
- They are created by very rich people that invest their own money.
- They don't make any money, they work as volunteers.

25) Which one of these online services is financed mostly by donations?

- **Wikipedia (online encyclopedia).**
- Facebook (social network).
- Google (search engine).
- Yahoo! (email service).
- Youtube/Dailymotion (video streaming).

26) Which of these propositions is false? A strong password should:

- **Be found in a dictionary.**
- Be at least 8 characters long.
- Combine letters, numbers, and symbol characters.
- Be changed regularly.
- Be unique for each of your online accounts.

27) You are most likely to meet strangers with ill intentions online on:

- **Open/random chat rooms or apps.**
- Social networks.
- Instant Messaging apps.
- Blogs.

28) Which one of these is an IP address?

- **192.0.81.250**
- www.deletecyberbullying.eu
- #DeleteCyberbullying
- @DeleteCyberbullying
- info@deletecyberbullying.eu

29) What information is never included in a photo that you have taken with your smartphone?

- The size of the picture.
- The date and time it was taken.
- The exact GPS location where it was taken.
- **Your mobile phone number.**
- Which lens was on your smartphones' camera.

30) Is it important to think before you "like" a Facebook page?

- No, it's harmless. I can like as many pages as I want.
- **Yes, not all Facebook pages can be trusted.**

Questions in the “Have you experienced” section

1) Do you talk with your parents about your online activities?

- Yes, I talk with them regularly.
- Yes, sometimes.
- Yes, I talk with them about some things I do online but there are topics that I wouldn't talk about that are too private.
- No, never.

2) (Have you experienced) Signing on to an online account and finding out the password was changed?

- Yes, it has happened to me several times.
- Yes, it has happened to me once or twice.
- No, but it has happened to a friend of mine.
- No, never.

3) Finding out some of your secrets were shared online?

- Yes, it has happened to me several times.
- Yes, it has happened to me once or twice.
- No, but it has happened to a friend of mine.
- No, never.

4) Seeing embarrassing material (pictures, videos, posts...) about you shared online?

- Yes, it has happened to me several times.
- Yes, it has happened to me once or twice.
- No, but it has happened to a friend of mine.
- No, never.

5) Being talked into sexting (sharing pictures, videos or comments of a sexual nature) by your friends, boyfriend or girlfriend who then shared it with others?

- Yes, it has happened to me several times.
- Yes, it has happened to me once or twice.
- No, but it has happened to a friend of mine.
- No, never.

6) Being entered/registered in a competition or poll (for instance if you're hot or not) without your permission?

- Yes, it has happened to me several times.
- Yes, it has happened to me once or twice.
- No, but it has happened to a friend of mine.
- No, never.

7) Posting material (pictures, videos, comments, messages...) about someone without his/her consent?

- Yes, I've done it several times.
- Yes, I've done it once or twice.

- One of my friends has done it.
- No, never.

8) Pretending to be one of your schoolmates or another person online?

- Yes, I've done it several times.
- Yes, I've done it once or twice.
- No, I've never done it.

9) Excluding someone from an online group/community or having been excluded from an online group that you wanted to be a member of?

- I've excluded someone from an online group/community.
- I've excluded someone because of his/her negative behaviour.
- I've been excluded by a moderator.
- I've been excluded by the other regular members of the group.
- I've both excluded someone and been excluded.
- I've witnessed it happening.
- None of the above.

10) Is it an advantage or a disadvantage to be anonymous online?

- More of a disadvantage because anonymous people harassed me and I felt powerless.
- More of an advantage because I can do what I want online, even harass people and stay anonymous.
- More of an advantage because by being anonymous, I can protect myself from many things including cyberbullying.
- Anonymity can be both good and bad. It depends on the situation.
- I have no opinion on this matter.

11) Modifying a picture or a video of someone without his/her consent and shared it online?

- Yes, I've done it several times.
- Yes, I've done it once or twice.
- No, I've never done it.

12) If you have harassed anyone online or if you would engage in harassment, why would you do so? (Multiple choice)

- It's nothing serious, just a joke.
- I did it for revenge.
- Everyone is doing it, I just followed.
- I was angry or upset about something.
- I had to, otherwise I would have been excluded or targeted next.
- I was bored...
- It's easier than bullying and I can remain anonymous.
- Other reasons.
- I would never cyberbully anyone.

Cyber-bullies could face two years in jail under new internet troll rules

ANNEXE 2:

A change to the criminal justice bill would target abuse on the internet or via mobile phones in England and Wales

Samuel Gibbs

Follow @SamuelGibbs Follow @guardiantech

theguardian.com, Wednesday 26 March 2014 13:24 GMT



The justice secretary has backed an amendment to the criminal justice bill that would target new rules at combating trolls. Photograph: Image Source/Getty Images

People convicted of cyber-bullying and text message abuse could face up to two years in prison, under plans backed by the government.

The justice secretary, Chris Grayling, has backed an amendment to the criminal justice bill that would target new rules at combating trolls that sexually harass and verbally abuse people on the internet or via mobile phones in England and Wales.

The amendment, due to be discussed in parliament on Thursday, was proposed by the Conservative MP for Ealing Central and Acton Angie Bray, after one of her constituents said her 14-year-old daughter had been “verbally raped” by 2,000 obscene texts sent by an older man, who escaped conviction.

“Just tabled amendment to criminal justice bill to make life just a bit harder for cyber-bullies and sex pests using texts to harass victims,” said [Bray on Twitter](#).

Crown court upgrade

The amendment would allow for greater penalties of up to two years in prison and extend the period of time made available to authorities attempting to build difficult cases against offenders.

Offences such as internet trolling fall under the Malicious Communications Act, which can only be tried in a magistrates’ court.

Bray’s tabled amendment comes after a string of high-profile abuse cases involving Twitter and text messages. Two abusers of the feminist campaigner Caroline Criado-Perez [were jailed in January](#) for subjecting her to threats of violence and rape on Twitter after Criado-Perez launched a campaign for more women to be represented on banknotes.

Criado-Perez [were jailed in January](#) for subjecting her to threats of violence and rape on Twitter after Criado-Perez launched a campaign for more women to be represented on banknotes.

The Labour minister for culture, media and sport, Helen Goodman, [called for “a clear legal framework”](#) to tackle the problem of cyber-bullying and the suicides of vulnerable young people in January, after the deaths of the teenagers Tallulah Wilson and Hannah Smith.

[Wilson died in 2012](#) aged 15 when she was hit by a train. An inquest into her death found that she had developed an alternative fantasy life online. In 2013, 14-year-old [Hannah Smith was found hanged](#) after being bullied on the open-discussion site Ask.fm.

A committee will discuss the [tabled amendment in parliament on Thursday](#), which will be added to the changes to laws to be voted on this year.

Facebook remark teenager is fired

A 16-year-old girl from Essex was fired after she described her office job as "boring" on her Facebook page.

Kimberley Swann, 16, of Clacton, had been working at Ivell Marketing & Logistics, in Clacton, for three weeks before being fired on Monday.

"I think they've stooped quite low," she said.

The firm's Steve Ivell said of the decision: "Her display of disrespect and dissatisfaction undermined the relationship and made it untenable."

Miss Swann said: "You shouldn't really be hassled outside work. It was only a throw-away comment.

" She says Clacton is boring but we're not going to throw her out of the house for it "
Janette Swann

"I came home from work one day, sat on the computer and said something about my job being boring."

Details were passed to her employers after she allowed colleagues access to her page, Miss Swann said, adding that she was not given the chance to explain.

Her mother, Janette, 41, said: "I think she's been treated totally unfairly. She didn't mention the company's name.

"This is a 16-year-old child we're talking about. She says Clacton is boring but we're not going to throw her out of the house for it."

Mr Ivell said: "Ivell Marketing is a small, close-knit family company and it is very important that all the staff work together in harmony.

"Had Miss Swann put up a poster on the staff notice board making the same comments and invited other staff to read it there would have been the same result."

TUC general secretary Brendan Barber said employers needed "thicker skins" in relation to social networking websites.

He said: "Most employers wouldn't dream of following their staff down the pub to see if they were sounding off about work to their friends."

Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/england/essex/7914415.stm

Published: 2009/02/27 13:44:22 GMT

© BBC 2014

ANNEXE 3b:

Facebook 'Friend' Robs Home Of Vacationing Family: Cops

The Huffington Post | By David Moya

Posted: 03/31/2014 2:31 pm EDT | Updated: 03/31/2014 5:59 pm EDT



This story won't get many "likes."

A woman on vacation in Las Vegas had [her house burglarized by a trio that allegedly included one of her Facebook "friends."](#)

Stacey Grant of Fontana, Calif., was so excited about her family's spring break trip to Sin City that she posted lots of social media updates about her whereabouts.

One of her Facebook friends apparently really "liked" those updates.

Investigators say Michael Batson, 21, used Grant's Facebook posts to case her home and, with the help of two other men, ransack it last Tuesday.

"It was hurtful," Grant told KNBC-TV. "My whole room was trashed, there were clothes everywhere. My bed was gone."

The alleged burglar even messaged Grant after her first Vegas post asking about her Vegas plans, according to her mom, Lavern Cheateam.

"Somebody she knew ended up texting her to make sure we were there, [asking her when were we coming back](#), how long we're going to be there," Cheateam told KABC-TV.

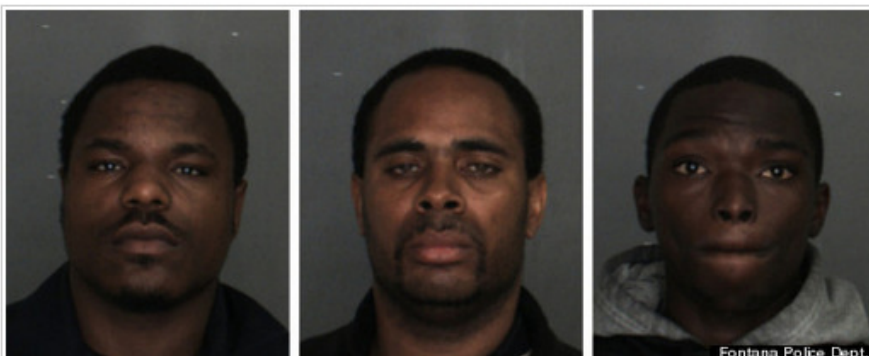
Luckily for the family, police caught the burglars in the act while doing some undercover surveillance around 3:30 a.m.

Officers spotted three men taking items out of the family's house and putting them into a U-Haul truck. The trio of [social media-savvy crooks fled the scene](#) -- one in the moving truck -- but were caught a short time later, the Press-Enterprise reports.

The officers found various items stolen from the house, including several flat-screen televisions and furniture.

Besides Batson, police arrested Phillip McKnight, 32, and Tyrone Gibson, 20. They were all charged with burglary, possession of stolen property and conspiracy.

The belongings are back, but Cheateam tells KABC-TV that she and her family will no longer post online about their vacations until they've returned home.



Missed call from someone you don't know? Phishing scam sees cell phone users charged if they call back numbers they don't recognise

- Conmen ring and hang up hoping a victim will call back
- Victim is charged sky-high international rate to be connected
- Calls tend to originate from the Caribbean, according to experts
- Scam is on the rise, according to experts

By TOM GARDNER

PUBLISHED: 14:07 GMT, 3 February 2014 | UPDATED: 16:14 GMT, 3 February 2014

Criminal gangs may have netted a fortune from a phishing scam which involves unsuspecting victims calling back unknown missed numbers.

In the so-called 'one-ring phone scam', a computer operated by a conman will dial a number and leave a missed called.

Victims who try to return the call are then redirected to an international adult entertainment service, 'chat' line, or other premium service located outside the country.

Those who fall for the ploy end up paying a \$19.95 international call fee, plus a \$9 per minute rate - sometimes more.

Authorities have now warned the scam may be on the rise as criminals take advantage of people's curiosity.

It is thought a handful of criminals could be bombarding thousands of phone numbers with the scam using computer programs.

Calls typically originate from outside the United States, according to the [Better Business Bureau](#).

One victim said her caller ID indicated the call originated in Antigua or Barbuda (area code 268). Other consumers across the country report calls from the Dominican Republic (809), Jamaica (876), British Virgin Islands (284) and Grenada (473), the [Better Business Bureau](#) reported.

The Federal Trade Commission (FTC) and Federal Communications Commission (FCC) have reviewed thousands of complaints about the practice, and expect the problem to grow.

Anyone who receives an unfamiliar out-of-state telephone number is advised to ignore it and not to call back.

People are also being urged to check their phone bills and alert their provider if they spot any unusual charges on the bill.



Scam: A phishing scam in which conmen leave a missed call and charge high rates when a victim calls back is on the rise (Stock picture)

ANNEXE 3d:

Smartphones Have Ruined Our Ability to Make Wasted Fools of Ourselves



Sam Biddle

Filed to: NSFW 3/27/13 4:00pm

116,693 🔥 2 ★



The modern smartphone, for all its utility as a way of capturing crimes in process, waddling babies, and public disasters, has one chilling effect on society: it's now dangerous to get insanely fucked up in public. And that's a damn shame.

Take this gentlelady at Miami's ULTRA music festival, a carnival of tacky bass, gaudy colors, and MDMA, who took to making out with a tree. Why? Because she was likely on some horrific cocktail of drugs, alcohol, and dubstep. We're not sure which of the three is the most toxic, but the combination is clearly potent. She takes off her pants and tries to have sex with a tree! This wouldn't work for reasons of physiognomy, genetics, and cultural mores, but she sure tries. She tries because, man, she wanted to. She was at a music festival, she was blitzed into the stratosphere, and she wanted that tree. She wanted to have sex with that tree, and she wasn't hurting anyone, and we live in a liberal democracy that's shed a lot of its Puritan restraint.

But this woman can't do what she likes without being YouTube shamed. It's impossible for her, or anyone else with some pills and a dream, to live free. To live free, and young, and without care. At the slightest provocation, you're guaranteed a league of smartphone surveillance and immediate sharing. You'll be uploaded in a flash. Your private moment of arboreal bliss transforms into so many views that the video is taken down and then re-uploaded multiple times.

The consequence is that we're all a little less fun—or headed that way. Within 15 seconds, even the slightest indiscretion, spilled drink, or untucked shirt can be recorded and texted or Instagrammed about. Our phones are better in the dark than ever before. They'll only get better. And once we're not safe to be silly in complete beer-darkness, we'll be skittish. Tense. Paranoid. And we'll be hypocrites, too: shame-shots get thunderous likes across social media, so we're at once turned on by exposing our friends' missteps, and terrified of making our own.

We don't even have Google Glass yet.

Imagine if they'd had smartphones at Woodstock? Would we be watching videos of our parents having sex and staring at clouds? Probably not, no—they'd be too worried about winding up on Reddit. So thanks, us, for making us too anxious to have horrific fun.

Like 389

2 ★ 209 Reply

36

ANNEXE 4: how to protect your privacy online⁷

1) *They ask, You don't tell*

Just because they ask, you don't have to tell. If you are just setting up an email account, you don't need to have a comprehensive profile. And if you are joining a social network, you can limit the amount of personal info you give out to the minimum. You can always make up an email address if you do not need a reply.

2) *Cookies are Best when you can eat them*

Make sure only the websites you visit will be able to collect information in the form of cookies by setting your browser to reject third party cookies. This way you can reduce the chances of the info being stolen by unscrupulous trackers, for example, via false adverts embedded on websites you visit.

3) *Passwords not passports*

Make sure your passwords keep your data safe and are not passports into your personal details. Don't use the same password everywhere, don't use a username on one site as a password for another. Hackers can cross-reference. Do use numbers and letters, some in capitals, in combinations that are not dictionary words.

4) *You give it away for others to sell it*

Dig a little and take a look at other people's profiles - what you can read about them, others can read about you. Posting pictures can also mean trouble. Once you've put your personal photos online you have very little control over how they are used. Still want to fill in all those details?

5) *Keep your personal data under lock and key*

Social networking sites are a goldmine for data-harvesters, so make things tough for them by setting your profile to the strictest privacy options. In a heated debate you may let slip more than you realise, so check what you are posting to make sure no personal details have slipped through.

6) *Close one door before you open the next*

Leaving yourself logged in to a social network or bank account is like leaving your car unlocked: you are wide open to infiltration by hackers. So avoid the risk and log out of accounts before surfing.

7) *Who's hitching a ride on your network*

If you are using a WiFi network make sure you don't have any hitchhikers along for the ride. Secure your network with a robust password and where possible use WPA encryption as this is stronger.

8) *Security, it's a two way street*

You keep your computer safe, you pay attention to your online details, but what about the people who are storing your info? You may have selected the highest security settings, but if a site can't keep your info safe, then you are still vulnerable. How trustworthy are the site owners and their own security systems?

9) *Damage limitation*

Consider using a payment method that is just for online shopping. Set a low credit limit: then if someone does get your card details, there's only so much damage they can do

10) *The large print giveth and the small print taketh away*

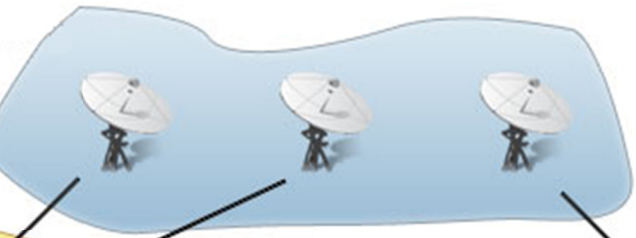
As true online as it is elsewhere, make sure you know what you are signing up to. For example, some contracts are auto renew and you have to opt out at a certain time if you don't want your credit card to be debited.

⁷ <http://www.europarl.europa.eu/news/en/news-room/content/20131003STO21413/html/How-to-protect-your-privacy-online>

The internet

ANNEXE 5:

Satellites



Data centers



The Backbone



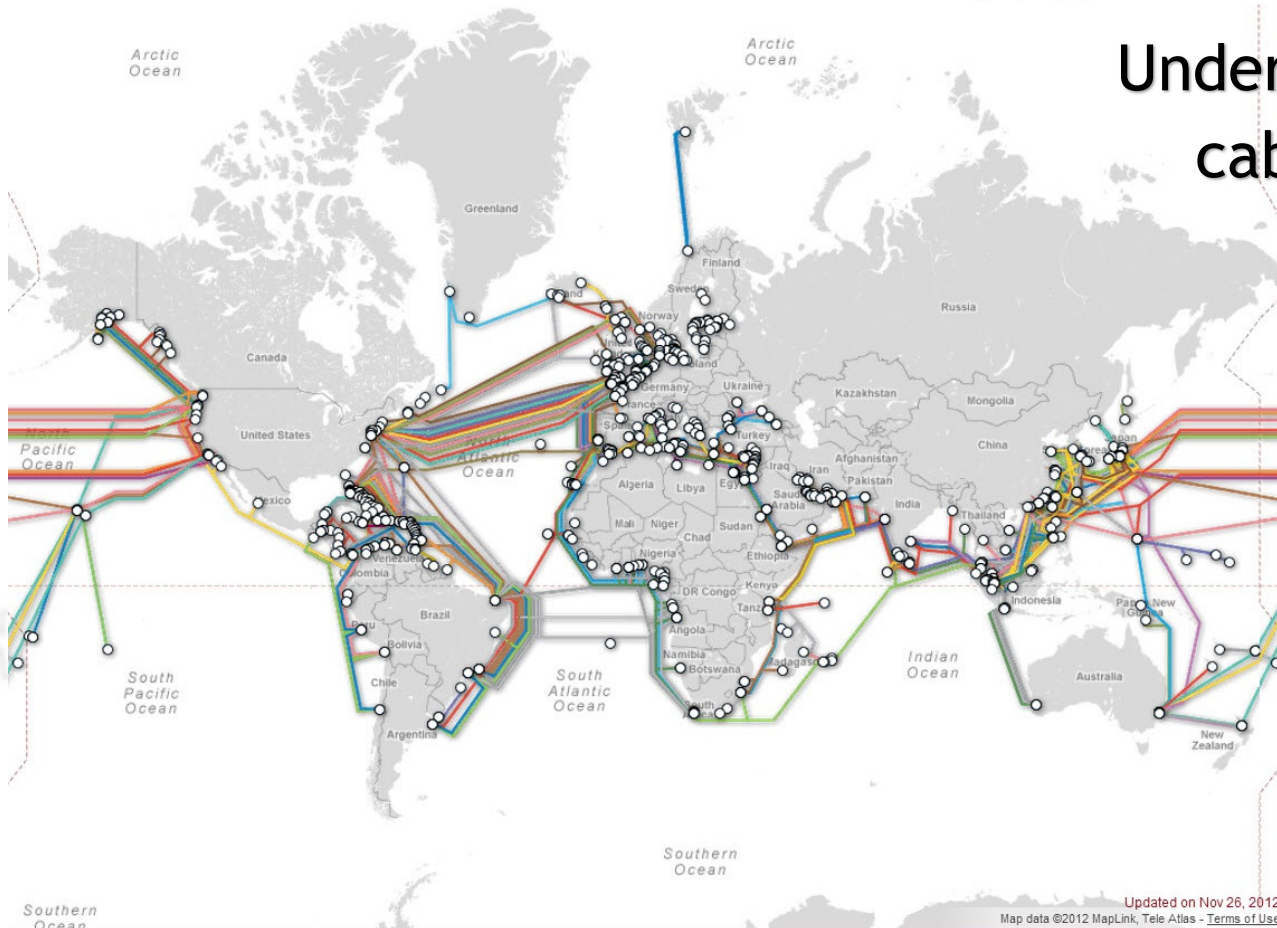
Local ISP



Users



Underwater cables



Southern Ocean

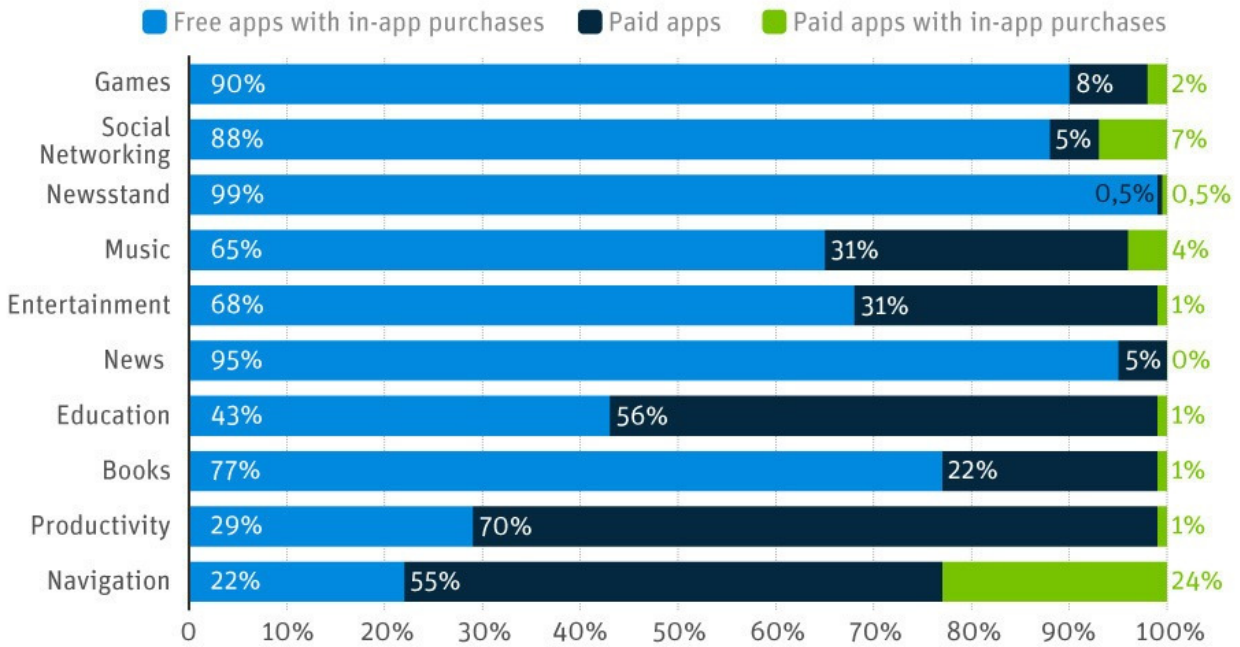
Southern Ocean

Updated on Nov 26, 2012
Map data ©2012 MapLink, Tele Atlas - Terms of Use

ANNEXE 6:

Freemium is the No.1 Pricing Strategy in Most App Categories

% of revenue generated in Apple's App Store from January through November 2013, by app category and pricing model



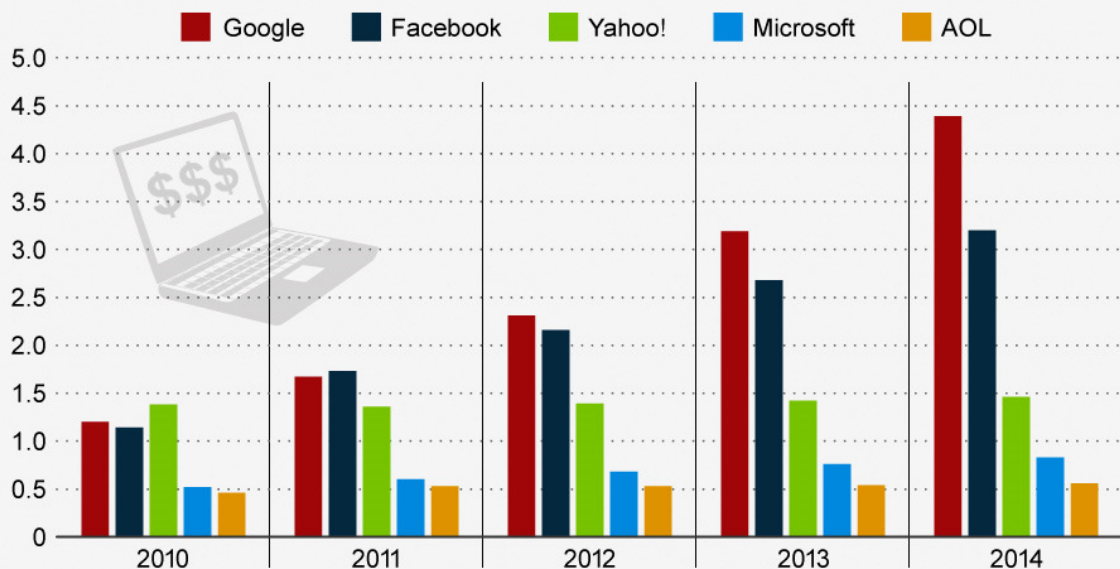
statista
The Statistics Portal

Mashable

Source: Distimo

Google and Facebook Set to Dominate Display Ads

Estimated U.S. display advertising revenue (in billion U.S. dollars)



statista
The Statistics Portal

CC creative commons

Source: eMarketer

ANNEXE 7:



Me You June 23, 2013

A person wearing a white tank top with the words 'FOREVER' and 'TOGETHER' is holding two red cans. The can on the left is labeled 'Me' and the one on the right is labeled 'You'. Both cans have the text 'Share a Coke with' above the name.

Like · Comment · Share 4

Today's Hot Contest

Win an iPad

An iPad is shown at an angle. The screen displays a video of a young boy with a wide smile, wearing a red and white shirt. A smaller video thumbnail is visible in the top left corner of the iPad screen.

Enter Your Cell Number

Go

Prior to qualifying for your prize, you'll be presented with optional third party offers. You do not need to complete these offers in order to receive your chance to get a prize.

DMCA / Terms / Privacy © 2011. All Rights Reserved.

CREDITS AND SOURCES:

<http://screwsandmarbles.wordpress.com/2013/06/14/tor-is-not-magic/>

<http://www.softicons.com/web-icons/web-hosting-icons-by-heart-internet/data-center-icon>

<http://www.sweetmaps.com/blog/wp-content/uploads/2012/11/submarinecablemap.jpg>

<http://www.boostingecommerce.com/e-commerce-trends-and-statistics-in-europe>

http://www.international-television.org/tv_market_data/online-advertising-world-usa-europe_2005-2012.html

<http://mashable.com/2013/12/19/paid-vs-free-apps/>

<http://www.statista.com/chart/620/estimated-display-advertising-revenue-of-major-digital-ad-selling-companies-in-the-united-states/>

<http://www.tnooz.com/article/google-versus-facebook-from-an-advertising-perspective-infographic/>

<http://yourstory.com/2014/03/ultimate-master-list-revenue-models-web-mobile-companies/>

<http://latticeclabs.com/blog/2013/09/premium-freemium-subscription/>

<http://jimshowalter.blogspot.be/2012/02/comparison-of-various-software-revenue.html>

<http://www.fastcompany.com/1768119/do-social-networks-really-compete-google-vs-linkedin-round-one>

<http://www.forbes.com/sites/erikkain/2013/05/09/as-world-of-warcraft-bleeds-subscribers-free-to-play-is-already-winning-the-future/>

http://www.gamasutra.com/blogs/SheldonLaframboise/20130806/197655/Why_Freemium_Feels_So_Damn_Good_in_League_of_Legends.php

<http://blogs.wsj.com/cmo/2014/07/15/okes-personalized-marketing-campaign-gains-online-buzz/>

ADDITIONAL INFORMATION:

The #DeleteCyberbullying project is funded by the DAPHNE III Programme of the EU Commission and has been coordinated by COFACE⁸.

According to the European Commission, **Cyberbullying** is repeated verbal or psychological harassment carried out by an individual or group against others. It can take many forms: mockery, insults, threats, rumours, gossip, “happy slapping”, disagreeable comments or slander. Interactive online services (e-mail, chat rooms, instant messaging) and mobile phones have given bullies new opportunities and ways in which they can abuse their victims.

Several objectives of the #DeleteCyberbullying project :

A **general acknowledgement** that cyberbullying is a real and substantial danger and causes immediate and significant harm.

An **exchange of best practice** about recognition, monitoring and prevention of harmful on-line communication and cyberbullying, especially in schools and families.

Specific recommendations to policy and decision makers at EU and Member States levels - Examples of prevention campaigns with positive impact.

Development of an on-line campaign material and **encourage the involvement of children** and young people, who we want not only to be the end-beneficiaries of the project, but to take ownership in the issue, and be part of the social and behavioural change we would like to create.

For more information about the project, visit our page www.deletocyberbullying.eu or send us an email at secretariat@coface-eu.org

DISCLAIMER:



This manual has been produced with the financial support of the DAPHNE III Programme⁹ of the European Union. The contents of this manual are the sole responsibility of COFACE and can in no way be taken to reflect the views of the European Commission.

⁸ www.coface-eu.org

⁹ http://ec.europa.eu/justice/grants/programmes/daphne/index_en.htm

LICENSE:



You are free:

- to copy, distribute, display, and perform the work.

Under the following conditions:



Attribution. You must attribute the work in the manner specified by the author or licensor.



Noncommercial. You may not use this work for commercial purposes.



No Derivative Works. You may not alter, transform, or build upon this work.

Your fair use and other rights are in no way affected by the above.