COMMUNICATION & SOCIETY

Horizontal surveillance, mobile communication and social networking sites. The lack of privacy in young people's daily lives

Alberto Hermida
https://orcid.org/0000-0003-4155-0108
ahermida@us.es
Universidad de Sevilla

Víctor Hernández-Santaolalla
https://orcid.org/0000-0002-2207-4014
vhsantaolalla@us.es
Universidad de Sevilla

Submitted
February 21st, 2019
Approved
October 17th, 2019

Communication & Society
ISSN 0214-0039
E ISSN 2386-7876
doi: 10.15581/003.33.1.139-152
www.communication-society.com

2020 – Vol. 33(1)
pp. 139-152

How to cite this article:
Hermida, A. & Hernández-Santaolalla, V. (2020). Horizontal surveillance, mobile communication and social networking sites. The lack of privacy in young people's daily lives. *Communication & Society, 33*(1), 139-152.

Abstract

Social networking sites and mobile communication have progressively encouraged the proliferation of certain surveillance and control practices employed by users on a daily basis. Platforms like Facebook and Instagram and devices such as mobile phones have normalised forms of horizontal surveillance, which have begun to be accepted by citizens as the norm. Thus, this paper examines a series of lateral and social surveillance practices that demonstrate a more deliberate and reprehensible behaviour on the part of users by focusing on the conflicts arising from the lack of privacy and control and the deficient management of inappropriate or annoying content in the social networking site environment. To this end, 311 students of the Universidad de Sevilla aged between 18 and 26 were asked to fill in a questionnaire. The survey results show that the majority of the respondents acknowledged having felt being spied on social networking sites, as well as having ended up at loggerheads with acquaintances as a consequence of having shared personal content with others. Lastly, it is apparent that, despite present concerns about the absence of privacy and control and inappropriate or annoying content, users believe that these are risks well worth running for the sake of sharing on social media.

Keywords
Social surveillance, lateral surveillance, social networking sites, mobile communication, privacy, control, content management.

1. Introduction

1.1. *Within the "empire of surveillance"*

Surveillance as a means of social control has evolved significantly since Jeremy Bentham developed the concept of the "panopticon" in his architectural prison design at the end of the eighteenth century. This concept, formalised "in developing his pragmatic theory of criminal law as the right to punish" (Mattelart, 2010, p. 7), was devised by Michel Foucault (1975) as the paradigm of the "disciplinary society," in which the body of the individual was disciplined and surveillance was conceived as a means of taming. Decades later, Foucault introduced the "security society" concept which, integrating its forerunner (Mattelart, 2010, p. 8-9), ceased

to act on the body of the individual in order to do so on society as a whole by breaking isolation and extending borders.

This has favoured the transition towards the so-called "empire of surveillance," according to Ignacio Ramonet (2015), in which digital control has followed in the footsteps of the physical kind (p. 81), becoming in turn both clandestine and massive. In his enlightening essay, the author dissects the power strategies aimed at intensifying surveillance and at undermining the protection of privacy, using to this end the fear of a terrified society as an exceptional weapon. In the realm of the Internet, "surveillance has become omnipresent and totally immaterial, imperceptible, undetectable, invisible. Moreover, it already is, on a technical level, exceedingly simple" (p. 11-12). In this context, in which the "unprecedented alliance" between the state, the military and the major Internet industries has helped to shape that empire of surveillance (p. 15), the development of information and communication technologies (ICTs) has gone a long way to consolidate the practice of mass spying.

In the era of democratised hyperconnectivity, in which spy software is generally available and user habits are even registered on the Internet of Things (IoT), surveillance is fundamentally focused on more technological information than on the human information (p. 95). Thus, Big Data and Big Brother converge under the pretext of creating a "safer" world; "surveillance-security: two concepts, one society" (Mattelart, 2010, p. 8). Likewise, with mobile communication in full swing, to the transformation of the average citizen's communication habits must be added the omnipresence of optimal surveillance tools, characterised not only by the immediacy with which they can be used, but also by being permanently connected.

In this sense, besides the vertical surveillance practices, there are also horizontal ones developed among the users themselves. Accordingly, this paper examines the horizontal surveillance dynamics among undergraduate students in relation to their daily use of social networking sites (SNSs) and mobile communication. Specifically, it takes an empirical approach to the Spanish university context, focusing on student practices and the conflicts deriving from privacy and content management issues.

1.2. *The two sides of citizen empowerment*

Citizens equipped with the necessary resources to conduct surveillance in two directions –vertical and horizontal– have become progressively more empowered. Regarding the former, the power pyramid has been inverted (McGrath, 2004, p. 198; Krona, 2015, p. 217), redirecting the vertical nature of surveillance process, with the individual now being able to "control" state forces. Through these dynamics of counter-surveillance, or "sousveillance" (Mann, Nolan & Wellman, 2003), the singularity of the "panopticon" is being substituted by the plurality of its participatory version (Cascio, 2005; Newell, 2014): the "catopticon" (Ganascia, 2010).

Thus, for example, the multiple gaze of the citizenry, equipped with mobile phones and other devices, registers, shares and reports any irregular activity in the power structures. Therewith, and in light of the development of "alternative journalism" (Poell & Borra, 2011; Poell & van Dijck, 2015), performed by citizens (Penney & Dadas, 2014) often with a smartphone and its different apps (Newell, 2014), state security services are exposed and visible online worldwide (Goldsmith, 2010; Penney & Dadas, 2014). It should come as no surprise then that countries like Spain have banned photographing or filming the police, as well as enacting legislation with severe penalties for those who do (Organic Law 4/2015 of 30 March, popularly known as the Gag Rule), as a remedial measure to curb this "excessive" vulnerability.

As regards horizontal surveillance practices (Albrechtslund, 2008), moreover, citizens themselves have different reasons for exercising peer-to-peer control and do so resorting to diverse mechanisms, thus developing one of the most unique features of present-day society,

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

as will be discussed in the following section. As summarised by Ignacio Ramonet (2015), "one of the anomalies of our societies of control is this: to make citizens both watchful and watched at the same time. Each should spy on the other, while being spied upon in turn" (p. 89).

So, citizen empowerment ultimately conceals a strategy which delves even deeper into the "empire of surveillance" concept, which limits the privacy and anonymity of individuals (Tello, 2013, p. 208; Hermida & Hernández-Santaolalla, 2016). In point of fact, the tools and devices that serve to conduct both vertical and horizontal surveillance are precisely those that allow the powers that be and major Internet corporations to achieve even greater control over user information, down to the smallest detail, profiting in turn from the data that they gather ("dataveillance"). Citizens now not only become their own spies, thus facilitating the work of those interested in their information, but also leave a digital footprint, allowing access to their personal privacy and constant tracking. Our activities generate data which are "collected, stored, monitored, shared, and sold by social media services, other online platforms, data brokers, intelligence agencies, and public administration" (Hintz, Dencik & Wahl-Jorgensen, 2017, p. 731). Under the premise of immediacy and convenience, the payment of bills or even the unlocking of devices using facial recognition can be achieved with exclusive, individual gestures... at the expense of priceless personal information. Each mobile phone, each application, each time geolocation features are activated and each item of shared content, among many other variables, is the piece of a puzzle which not only analyses individuals in their private space, but also maps all their movements. In that regard, datafication "provides vastly enhanced possibilities to understand, predict, and control citizen activities" (p. 732), all of that in an environment dominated by the so-called "surveillance capitalism" (Zuboff, 2015, 2019). This surveillance capitalism becomes a market force that, through this huge collection of information, could ultimately annihilate the freedom of choice and the freedom of market praised by capitalism. Furthermore, this compilation of information would have a certain support by the citizens, who –not exempt from certain ignorance because of the unprecedented of the situation– are willing to transfer private information if this gives them a better and easier use of technology, as well as greater and faster, as well as personalized, access to information.

1.3. *Surveillance and SNSs*

In this context of continual expansion, the development of ICTs and the subsequent transformation of users' communication habits have led to the adoption of different forms of horizontal surveillance, conditioned by the centrality of the Internet in society and in everyday life. Therefore, in a scenario in which the "extimacy" or the sharing of personal information on SNSs is now the norm (Tello, 2013), a number of relevant studies have recently been conducted on the different search, surveillance and control dynamics/strategies implemented by users. Numbering among these, included under the umbrella nomenclature "interpersonal electronic surveillance" (IES) (Tokunaga, 2011), are terms such as "lateral surveillance" (Andrejevic, 2005), "participatory surveillance" (Albrechtslund, 2008), "mobile surveillance" (Ngcongo, 2016) and "social surveillance" (Steinfield, Ellison & Lampe, 2008; Tokunaga, 2011; Marwick, 2012).

From Andrejevic's (2005) approach, "lateral surveillance" or "peer-to-peer monitoring" implies "the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another" and covers three basic categories: "romantic interests, family, and friends or acquaintances" (p. 488). Specifically, these practices are closely related to "the democratization of access to the technologies and strategies for cultivating investigatory expertise" (p. 482) and in consonance with the premise of "do-it-yourself private investigators" and its gradual introduction in society (p. 487). Therefore, Andrejevic's study focuses on the use of lie detectors (computer-driven and/or physical), the installation of hidden cameras at home and monitoring software on computers, as well as on

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

a wide range of online services which offer from background checking to re-territorialising mobile communications, through other options.

Similarly, besides these more sophisticated strategies, the "dark side" of SNSs (Shelton & Skalski, 2014) has become a popular object of study. In this connection, Fox and Moreland (2015) number among the negative psychological and relational experiences associated with SNSs, particularly Facebook stressors, "managing inappropriate or annoying content, being tethered, lack of privacy and control, social comparison and jealousy, and relationship tension and conflict" (p. 168). As regards daily peer control and surveillance, the pioneering works of authors such as Lampe, Ellison and Steinfield (2006) have been followed by important studies that connect SNSs to these practices (Albrechtslund, 2008; Fuchs, 2011; Trottier, 2012), especially in the context of romantic relationships (Marshall, Benjanyan, Di Castro & Lee, 2013; Tokunaga, 2011, 2016; Rus & Tiemensma, 2017; Wang, Zhou & Zhang, 2017). For his part, Tokunaga (2011) highlights four features of SNSs that favour IES: "accessibility, multimediation, recordability and archival, and geographical distance" (p. 707), before going on to underscore three potential factors influencing the development of IES on SNSs: demographic, relationship and Internet use variables (p. 707-708).

In the same line, Marwick (2012) has determined the characteristics of social surveillance and has analysed their implications in a series of specific case studies. According to the author, this type of surveillance is consistent with the use of Web 2.0 resources "to continually investigate digital traces left by the people they are connected to through social media" (p. 378). Specifically, for the author the main differences between this and the traditional form of surveillance, or its opposite ("sousveillance"), lie in three basic parameters: power, hierarchy and reciprocity. Regarding the first, "*social surveillance* assumes a model of power flowering through all social relationships." Based on hierarchy, it "takes place between individuals, rather than between structural entities and individuals." Finally, depending on the degree of reciprocity, Marwick states that "people who engage in social surveillance also produce online content that is surveilled by others" (p. 382). Furthermore, the very use of SNSs and the desire to share all kinds of content are tantamount to wanting to be seen by others (p. 390).

Taken to the extreme, the most pernicious side of these practices can lead to digital bullying and blackmailing, among other things. Nevertheless, the mere fact of introducing surveillance and control in daily life through SNSs like Facebook (Marshall, 2012; Tong, 2013; Fox & Warber, 2014) and Instagram (Sheldon & Bryant, 2016), and that these practices and their consequences can go unnoticed or are taken for granted by users, makes it necessary to continue exploring the nature of this growing social problem. Moreover, it should be borne in mind that with the proliferation of smartphones and other mobile devices, these practices have become universal, with hyper-accessibility easily becoming an obsession. In this regard, user privacy takes centre stage, due to the obvious risk of its continuous invasion and to users' concerns about its correct management. As a matter of fact, in a recent study that highlights the importance of these issues in the context of mobile communication, Ana Serrano-Tellería concludes that "users generally continued to lack proper abilities and capacities to manage their privacy consciously and properly," in spite of the "increased awareness and idea of the risks involved" (2018, p. 827). However, on the other hand, Casilli (2015) highlights that "claims that 'the end of privacy is nigh' are erroneous and ideologically motivated," in his theses on digital mass surveillance and the negotiation of privacy (p. 4). Specifically, and contrary to hypothesis of the end of privacy, "users are making increasingly insistent demands for autonomy and personal and collective empowerment" (p. 5). In fact, as the author points out, the increasing of encryption tools or the "amnesic" operating systems, among other resources, "are all clear indications of the growing interest for users' control over their online presence" (p. 5).

In view of the above, the main objectives of this study are to examine deliberate and reprehensible social and lateral surveillance practices employed by undergraduate students

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

at the Universidad de Sevilla. Additionally, in relation to SNSs and mobile communication, it explores the management of inappropriate or annoying content and the lack of privacy and control as the main psychological stressors.

2. Material and methods

In order to meet the established objectives, this study used a quantitative methodological approach. Following previous studies, such as those of Lampe *et al.* (2006), Marshall *et al.* (2013), Fox and Warber (2014) and Tokunaga (2011, 2016), an on-site survey was conducted from 15 to 19 May 2017. The respondents, who were all communication students (Ngcongo, 2016; Tokunaga, 2016) at the Universidad de Sevilla (Spain) aged between 18 and 26 years old (M=20.5; SD=1.9), spent, on average, 20 minutes to complete the questionnaire. Specifically, 319 respondents completed it and, once those with errors had been eliminated, the answers to 311 (198 female and 113 male respondents) were then analysed using IBM SPSS Statistics 24.0 statistical software.

Besides a number of sociodemographic control questions, the questionnaire, which had an acceptable reliability, α = 0.81, as shown by Cronbach's alpha, was divided into six main questions: two with 25 items measured on a five-point Likert scale; one yes/no (or nr/dk) question; and three open ones. In the first questions, the respondents were asked about the kind of (1) social and lateral surveillance practices that they employed and suffered (i.e. recording audio/video or taking photos of others and sharing them without their consent, or checking the profiles of people who were not their friends through others who had them in their contacts); and how (2) they managed their privacy and inappropriate or annoying content (i.e. checking the privacy settings of their SNS accounts or asking someone to delete personal content posted without their consent).

Regarding the practices employed or suffered by the respondents, it is important to clarify that the intention here was to inquire about certain actions that have been confirmed as habitual in previous studies and that can be understood as inherent to SNS use. On the contrary, the questionnaire was designed to analyse other more deliberate and conflictive surveillance practices that, generally speaking, obviously violated the privacy of others. This is why the questionnaire was not restricted to the study of social surveillance, but also included certain lateral surveillance practices linked to the use of SNSs and mobile devices, as well as to content sharing dynamics.

In relation to the open questions, the participants were asked to indicate SNS behaviours which they might have regretted and to point to practices that they themselves had suffered and considered especially offensive or intrusive. Finally, they were given the opportunity to make any comments or observations that they deemed appropriate. This allowed for the gathering data not covered by the previous questions and, in general, provided more qualitative information.

3. Results

In light of the clarifications offered above, it should be noted that none of the practices studied here were widely employed by the respondents (Table 1). However, although those practices that could be classified as more "extreme" were infrequent, some were recurrent enough to raise concern, due to their intrusiveness and excessive violation of privacy. For instance, some of the respondents recognised having developed practices such as using a webcam to record people without their permission or resorting to apps to track third-party mobile phones via geolocation. Other practices, in contrast, such as consulting the user profiles of those who are not "friends" via third parties, were very frequent, as admitted by 77.5% of respondents. Lastly, although less frequent, it is important to highlight the use of SNSs to threaten people. In this regard, 14.7% of the respondents acknowledged having threatened, at least once, to share someone else's personal content, while 20.0% claimed that this had happened to them

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

occasionally. What is also noteworthy is that 66.6% of the respondents had felt spied on by other users at some time or another. With respect to the sociodemographic control questions, gender was the variable that produced the greatest differences. By and large, the female respondents checked more frequently the SNS profiles of people who were not on their friend lists through third-party contacts ($\chi 2$ (4) = 11.0, $p<0.03$).

In relation to the management of privacy and inappropriate or annoying content (Table 2), it should be noted how, for example, 19.9% of the respondents had never disabled app geolocation features, while 38.6% of them regularly shared their location on SNSs or mobile apps. However, 64.0% of the respondents claimed to be aware of the geolocation features of their mobile devices. Although in none of the items a particularly remarkable frequency was obtained, the inadequate use of personal content by others without permission had led 71.0% of the respondents to ask others to delete content at least occasionally. In this case, there were also significant gender differences, with the female respondents more frequently sharing their location at any given moment on SNSs or mobile apps ($\chi 2$ (4) = 20.6, $p<0.001$) and asking others to delete content that affected them personally ($\chi 2$ (4) = 11.3, $p<0.03$). Indeed, for a 20-years-old girl an especially offensive/intrusive practice was "to upload photos of her without her consent and to refuse to delete them, when asked to do so."

Moving on to privacy management, the respondents were asked to answer "yes" or "no" to a number of questions relating to the legal terms and conditions that must be accepted to open an SNS account or to install an app. In this regard, 88.9% of respondents admitted to having not read the terms and conditions, while 66.9% were unaware of who had the rights to the images and videos posted on SNSs. However, 85.1% declared that they did indeed check the privacy settings of their accounts, which is remarkably inconsistent with the two previous findings. On the other hand, 38.5% conceded that they paid little or no attention to the accesses that apps requested during installation, while 21.6% even stated that they would install an app even though it requested excessive access to their devices. On this occasion, no significant differences were detected in relation to the sociodemographic variables.

Table 1: Social/lateral surveillance practices and user perception.

	Men		Women		Total	
	M	SD	M	SD	M	SD
Checking the profiles of people who are not my friends through others who have them in their contacts	3.17	1.11	3.54	1.10	3.40	1.12
Facilitating access to my friends' content to other people who do not have them in their contacts	2.47	1.17	2.82	1.28	2.69	1.23
Using personal content obtained from other accounts without permission	1.48	0.79	1.49	0.91	1.49	0.87
Saving the personal content of others for possible later use	2.24	1.26	2.30	1.33	2.28	1.30
Recording audio/video and taking photos of others and sharing them without their consent	1.99	1.23	1.93	1.14	1.95	1.17
Sharing photos/videos of others (in which I do not appear) without permission	2.07	1.22	2.02	1.27	2.04	1.24
Sharing audio/videos/photos recorded/taken by me with others without permission	2.05	1.39	1.93	1.14	1.98	1.23
Feeling threatened by someone who intends to share my personal content	1.28	0.75	1.37	0.79	1.34	0.78

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

Threatening to share someone else's personal content	1.21	0.62	1.25	0.69	1.24	0.64
Saving someone else's personal content in order to counteract possible threats	1.65	1.06	1.62	1.02	1.63	1.03
Reading conversations that my classmates or friends have had with other people	2.11	1.08	2.28	1.27	2.22	1.21
Using a webcam to record without permission	1.06	0.28	1.05	0.29	1.05	0.29
Resorting to mobile apps to track other people's mobile phones via geolocation	1.06	0.28	1.11	0.42	1.09	0.38
Having a peep at other people's accounts when I find an open session	1.79	1.01	2.02	1.31	1.94	1.22
Feeling uncomfortable seeing very personal content on my friends' profiles	2.60	1.28	2.93	1.29	2.81	1.29
Feeling guilty seeing very personal content on my friends' profiles	1.94	1.04	1.77	1.07	1.83	1.06
Feeling observed on SNSs	2.27	1.20	2.34	1.22	2.31	1.21

Source: Own elaboration based on data survey.

Table 2: Privacy/inappropriate or annoying content management.

	Men		Women		Total	
	M	SD	M	SD	M	SD
Using filters to limit the viewing of the content that I share	2.79	1.49	2.99	1.37	2.92	1.41
Asking someone to delete specific content that directly concerns me	2.23	1.27	2.74	1.35	2.55	1.34
Ending up at loggerheads with someone who has refused to delete content that directly concerns me	1.75	1.07	2.10	1.29	1.97	1.22
Arguing with friends, family or partners over any type of use of personal content	1.84	1.17	1.90	1.05	1.88	1.09
Trying to use tools to see who has checked my profile	1.88	1.16	2.02	1.27	1.97	1.23
Sharing my current location on SNSs or mobile apps	2.59	1.22	3.27	1.31	3.03	1.31
Reporting content that I consider offensive	3.06	1.33	3.18	1.53	3.14	1.46
Filtering which apps have access to my location	2.96	1.47	3.13	1.94	3.07	1.42

Source: Own elaboration based on data survey.

In the main, a certain degree of discrepancy between how SNSs are perceived and user behaviour was detected. In this connection, the sensation of being spied on was especially noteworthy and had a direct, albeit low, correlation with different practices apparently associated with social and lateral surveillance, and another pertaining to privacy and inappropriate or annoying content management (Table 3). Additionally, Table 4 shows the correlation between some premeditated social and lateral surveillance practices, such as saving the personal content of others for possible future use and actions aimed at preserving the privacy of personal content and the owner's control over it. In this regard, it is especially remarkable how this correlates positively, albeit not very intensely, with disputes with third parties over personal content; although, in any case, it is impossible to determine the order in which this occurs. In line with the quantitative data, and in relation to the survey's open questions, it is interesting that the most frequent answer to the question about what the respondents most regretted was stalking other people's profiles. This is a much more serious matter when people create "false profiles" in order to "spy on people" who have blocked them, as confessed by a 24-year-old male student. Similarly, other respondents suggested that they

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

felt remorseful not for having spied on others, but rather for having been discovered in the process or –when taking things too far– for having accessed information that they would rather not have discovered.

Apart from spying, other issues that caused the greatest regrets were sharing too much personal information ("in a way you wouldn't if you were not in front of a screen"), spending too much time connected and saving and/or sharing the private conversations and content of others without their permission. Lastly, it is interesting to note how some of the respondents regretted behaviour bordering on social exhibitionism or aimed at impressing their contacts. In this respect, a respondent claimed that she shared photos "because everyone else's doing it," while another lamented "having published content to impress people, without really wanting to do so." Similarly, a third participant regretted having "deleted photos that weren't popular enough." thus highlighting the narcissism, exhibitionism and vanity generally associated with SNSs.

Nevertheless, these practices must not merely be considered from the point of view of those who employ them, but rather from that of those who suffer them. Therefore, the third-party uses of personal content which the respondents considered to be particularly reprehensible or intrusive were sharing offensive material, threating to post personal content and even identity theft, as stated by nine respondents. Specifically, three of them claimed that someone had used their photos to create false accounts, while two others reported more serious cases of identity theft, namely, "impersonating them to share content on their behalf" (male, 21-years-old) and even "to generate offensive content" (female, 21-years-old). For her part, a 20-years-old female respondent directly mentioned the term "cyberbullying" as a persistent practice, finally contending that "nowadays it's very difficult for us to have complete trust in any social network site or app."

In this connection, some of the respondents ultimately criticised SNSs and the uses to which they were put, due to, for instance, "their increasingly obsessive and oppressive use" (female, 22-years-old). This led some of the respondents to yearn for the good old days when "face-to-face" communication was the norm (male, 25-years-old), to such an extent that one respondent (female, 22-year-old) longed "to return to the twenty-first century." In light of this, and in line with those respondents who believed that the problem lay more in their use than in technology itself, one respondent (male, 25-years-old) recommended that "the use of social media should be taught at school."

Table 3: Pearson's r correlation between social/lateral surveillance practices and user perception (n=311).

	Feeling uncomfortable seeing very personal content on my friends' profiles	Feeling guilty seeing very personal content on my friends' profiles	Feeling observed on SNSs
Checking the profiles of people who are not my friends through others who have them in their contacts		0.14*	0.18**
Facilitating access to my friends' content to other people who do not have them in their contacts		0.13*	0.16**
Using personal content obtained from other accounts without permission	0.15**	0.15*	
Saving the personal content of others for possible later use	0.23**	0.25**	0.30**
Saving someone else's personal content in order to counteract possible threats		0.14*	0.37**

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

Sharing photos/videos of others (in which I do not appear) without permission			0.14*
Threatening to share someone else's personal content			0.25**
Reading conversations that my classmates or friends have had with other people	0.11*	0.15**	0.23**
Ending up at loggerheads with someone who has refused to delete content that directly concerns me	0.15**		0.28**
Arguing with friends, family or partners over any type of use of personal content	0.18**	0.19**	0.40**
Using filters to limit the viewing of the content that I share	0.19**		0.16**
Asking someone to delete specific content that directly concerns me	0.22**		0.18**
Trying to use tools to see who has checked my profile			0.25**
Sharing my current location on SNSs or mobile apps	0.12*		
Reporting content that I consider offensive	0.17**		0.17**
Filtering which apps have access to my location	0.18**		

*Significant at the 0.05 level. ** Significant at the 0.01 level.

Source: Own elaboration based on data survey.

Table 4: Pearson's *r* correlation between privacy/content management and social/lateral surveillance practices (n=311).

	Saving the personal content of others for possible later use	Saving someone else's personal content in order to counteract possible threats	Threatening to share someone else's personal content	Feeling threatened by someone who intends to share my personal content
Asking someone to delete specific content that directly concerns me	0.19**		0.14*	0.12*
Ending up at loggerheads with someone who has refused to delete content that directly concerns me	0.24**	0.16**	0.14*	0.29**
Arguing with friends, family or partners over any type of use of personal content	0.24**	0.33**	0.29**	0.33*
Trying to use tools to see who has checked my profile	0.15**	0.19**	0.16**	
Sharing my current location on SNSs or mobile apps	0.28**	0.14*	0.20**	

*Significant at the 0.05 level. ** Significant at the 0.01 level.

Source: Own elaboration based on data survey.

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

4. Discussion and conclusions

SNSs and mobile communication have enabled the progressive normalisation of certain horizontal surveillance practices principally based on information gathering and monitoring among users. For that matter, studies such as those performed by Marwick (2012) and Trottier (2012), among others, have approached the dynamics assimilated by individuals from a qualitative perspective, revealing not only their level of involvement, but also their level of knowledge in this regard. In this context, the risk of excessive exposure and invasion of privacy has been accepted by users in the interest of visibility and the need to share (Serrano-Tellería, 2018). To such an extent, in fact, that the resulting exhibitionism has led to excessively narcissist and vigilant attitudes (Moon, Lee, Lee, Choi & Sung, 2016; Sheldon & Bryant, 2016).

In relation to the above and in light of the results obtained, although it is impossible to talk about a widespread use of practices that demonstrate a clear intention to violate the privacy of others or to bully them, the significant fact that the respondents admitted to having occasionally resorted to them is indeed food for thought. This points to how interpersonal surveillance encounters on SNSs and mobile devices the democratisation of a number of tools that introduce citizens into the "empire of surveillance" (Ramonet, 2015), encouraging them participate in a reality that gradually becomes integrated into their daily lives.

Likewise, beyond the practices employed, it is obvious that the respondents were concerned about their vulnerability in such an environment, as shown by the fact that two thirds of them admitted to having had the sensation of being watched on SNSs. This feeling not only underscores their experience and knowledge of the "dark side" of social media (Fox & Moreland, 2015), but also of their widespread use as platforms for spying on others and being spied on; a risk that they were apparently willing to take.

Consequently, such a feeling can be associated with the main stressors addressed in this study. On the one hand, it is linked to the lack of privacy and control and to concerns about the management of the former, with a view to being able to regulate access to certain content; and on the other, to the management of inappropriate or annoying content, particularly when it affects the individual identity of users. In this respect, 71% of the respondents acknowledged that, at one time or another, they had had to ask third parties to delete undesirable personal content that had been previously posted by them. And in some cases, this had even led to conflict with those who had shared the content. Moreover, as has been seen, some of the respondents had suffered from phishing, with unwelcome content having been posted on their behalf, a practice that has a huge impact on vulnerability and infringement of privacy.

At all events, the respondents were, by and large, more concerned about their personal content being accessed by other users than by major corporations, the consequences of the introduction of "dataveillance" (van Dijck, 2014) being of secondary importance. Unsurprisingly, 88.9% of them admitted to having ignored the legal terms and conditions when installing an app or opening an SNS account, accepting them without further ado.

Similarly, in an environment in which the sharing of personal photos is one of main reasons for using SNSs, it is remarkable that 66.9% of the respondents did not know who had the rights of the images and videos posted on such sites. In consonance with the study published by Serrano-Tellería (2018), the vast majority of the respondents in the adolescents focus group "gave up this right when uploading/putting photos online. The motivations for sharing suggested that the impetus for interaction was greater than concerns about the risk" (p. 825). In this respect, the respondents' concerns were apparently inconsistent, insofar as even though they confirmed that they did not read the terms and conditions before installing apps or opening accounts, they declared that they did indeed review the privacy policy of their account to a greater or lesser extent. This partially connect with the study of privacy in the age of information developed by Acquisti, Brandimarte and Loewenstein (2015). Specifically, the authors indicate that "62% of respondents to a survey believed (incorrectly) that the

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

existence of a privacy policy implied that a site could not share their personal information without permission, which suggests that simply posting a policy that consumers do not read may lead to misplaced feelings of being protected" (p. 512).

Furthermore, it should be noted that 38.5% of the respondents ignored the access permission requested by apps, while nearly 25% of them were perfectly willing to install an app in spite of the fact that it requested permission to set an excessive level of access to their mobile devices. All this stresses a degree of caution among users, putting the accent on individuals as the main risks as regards the invasion of privacy. For the respondents generally accepted the rules of the game established by social media corporations with little suspicion and as a necessary "sacrifice" in order to be able to avail themselves of their services. Nonetheless, some of them criticised the excessive control of the major SNS service providers.

With respect to the relationship between the feelings associated with the lack of privacy and control on SNSs and the horizontal surveillance practices discussed in this paper, it is only logical that "feeling spied on" correlated positively with being at odds with third parties for sharing personal content and refusing to delete posts. However, what is more interesting is the fact that such a feeling also correlated positively with saving the personal content of other users for its subsequent use should the opportunity arise, even for countering possible threats. This fact, in addition to broadening the knowledge of users of the harmful side effects of SNSs, buttresses the idea of a certain shift towards more drastic and deliberate interpersonal surveillance practices. Far from searching for information or peer monitoring on social media, among other more normalised practices, SNS-related conflicts reveal a number of worrying attitudes. In this regard, by interrelating the data shown in Tables 3 and 4, it seems that SNSs, mobile devices and horizontal surveillance are fast becoming scenarios of conflict and control, in which users are aware of the risks involved and, even when assuming them, are subject to potential stressors that can affect their daily lives.

Lastly, the results of this study indicate that the respondents were aware of the dangers posed by SNSs and mobile devices as surveillance and control mechanisms. Nonetheless, their concern about privacy management was exclusively restricted to the potential risks of this being invaded by other users. Only in a few cases was there real concern about personal data gathering by major corporations; a risk that, in any case, was assumed and relegated to second place.

5. Limitations and future research

This study has several limitations that should be borne in mind when interpreting the data. Firstly, although undergraduates have usually been selected as the study population in previous studies, the generalisability of the results is limited due to the fact that it is a university sample. Secondly, and tying in with this limitation, the respondents' experiences with SNSs and mobile devices might have been conditioned by the fact that they were communication students. Finally, the most frequent social surveillance practices have been, to some degree, taken for granted and excluded from the survey, due to both the conclusions of previous studies—cited in the text—and its approach focusing more on deliberate and reprehensible practices.

Although the findings reflect the respondents' experiences, further theorising and empirical research will be necessary in the context of more extreme horizontal surveillance practices. Specifically, some of the data obtained in this study raise the alarm over pernicious activities that should be monitored more closely in future studies.

The authors would like to express their gratitude to the former fellowship students of the Department of Audiovisual Communication and Advertising of the Universidad de Sevilla, Inmaculada Mármol Martín, Sara Mena Vega, and Sara Rebollo Bueno.

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). Retrieved from https://bit.ly/2cbeOWK

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479-497. https://www.doi.org/10.24908/ss.v2i4.3359

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. https://www.doi.org/10.1126/science.aaa1465

Cascio, J. (2005). The rise of the participatory panopticon. *World Changing*. Retrieved from https://bit.ly/2dQI6yw

Casilli, A. A. (2015). Four theses on digital mass surveillance and the negotiation of privacy. Paper presented at the 8th Annual Privacy Law Scholar Congress, Berkeley Center for Law & Technology, Berkeley, USA. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01147832

Foucault, M. (1975). *Surveiller et punir. Naissance de la prison*. Paris: Gallimard.

Fox J. & Moreland J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior*, *45*, 168–176. https://www.doi.org/10.1016/j.chb.2014.11.083

Fox, J. & Warber, K. M. (2014). Social networking sites in romantic relationships: Attachment, uncertainty, and partner surveillance on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *17*(1), 3-7. https://www.doi.org/10.1089/cyber.2012.0667

Fuchs, C. (2011). New media, web 2.0 and surveillance. *Sociology Compass*, *5*(2), 134-147. https://www.doi.org/10.1111/j.1751-9020.2010.00354.x

Ganascia, J. G. (2010). The generalized sousveillance society. *Social Science Information*, *49*(3), 489-507. https://www.doi.org/10.1177/0539018410371027

Goldsmith, A. J. (2010). Policing's new visibility. *British Journal of Criminology*, *50*(5), 914-934. https://www.doi.org/ 10.1093/bjc/azq033

Hermida, A. & Hernández-Santaolalla, V. (2016). Ambigüedades del empoderamiento ciudadano en el contexto tecnopolítico. *IC-Revista Científica de Información y Comunicación*, *13*, 263-280. Retrieved from https://bit.ly/2xGRaPs

Hintz, A., Dencik, L. & Wahl-Jorgensen, K. (2017). Digital citizenship and surveillance society. *International Journal of Communication, 11*, 731-739.

Krona, M. (2015). Contravigilancia y videoactivismo desde la plaza Tahrir. Sobre las paradojas de la sociedad contravigilante. In F. Sierra & D. Montero (Eds.), *Videoactivismo y movimientos sociales. Teoría y praxis de las multitudes conectadas* (pp. 211-232). Barcelona: Gedisa.

Lampe, C., Ellison, N. & Steinfield, C. (2006). A Face(book) in the crowd: Social searching vs. social browsing. *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*, 167-170. Retrieved from https://bit.ly/2zwbQLc

Mann, S., Nolan, J. & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, *1*(3), 331-355. https://www.doi.org/10.24908/ss.v1i3.3344

Marshall, T., Benjanyan, K., Di Castro, G. & Lee, R. A. (2013). Attachment styles as predictors of Facebook-related jealousy and surveillance in romantic relationships. *Personal Relationships*, *20*(1), 1-22. https://www.doi.org/10.1111/j.1475-6811.2011.01393.x

Marshall, T. C. (2012). Facebook surveillance of former romantic partners: Associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior, and Social Networking*, *15*(10), 521-526. https://www.doi.org/10.1089/cyber.2012.0125

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378-393. https://www.doi.org/10.24908/ss.v9i4.4342

Mattelart, A. (2010). *The Globalization of Surveillance*. Cambridge (UK): Polity Press.

McGrath, J. E. (2004). *Loving Big Brother: Performance, Privacy and Surveillance Space*. London (UK): Routledge.

Moon, J. H., Lee, E., Lee, J. A., Choi, T. R. & Sung, Y. (2016). The role of narcissism in self-promotion on Instagram. *Personality and Individual Differences 101*, 22-25. https://www.doi.org/10.1016/j.paid.2016.05.042

Newell, B. C. (2014). Crossing lenses: Policing's new visibility and the role of "smartphone journalism" as a form of freedom-preserving reciprocal surveillance. *Journal of Law, Technology and Policy*, *1*, 59-104.

Ngcongo, M. (2016). Mobile communication privacy management in romantic relationships: a dialectical approach. *Communication*, *42*(1), 56-74. https://www.doi.org/10.1080/02500167.2016.1140666

Penney, J. & Dadas, C. (2014). (Re)Tweeting in the service of protest: Digital composition and circulation in the Occupy Wall Street Movement. *New Media & Society*, *16*(1), 74-90. https://www.doi.org/10.1177/1461444813479593

Poell, T. & Borra, E. (2011). Twitter, YouTube, and Flickr as platforms of alternative journalism: The social media account of the 2010 Toronto G20 protests. *Journalism*, *13*(6), 695-713. https://www.doi.org/10.1177/1464884911431533

Poell, T. & van Dijk, J. (2015). Social media and activist communication. In C. Atton (Ed.), *The Routledge Companion to Alternative and Community Media* (pp. 527-537). London (UK): Routledge.

Ramonet, I. (2015). *El imperio de la vigilancia*. Madrid: Clave Intelectual.

Rus, H. M. & Tiemensma, J. (2017). "It's complicated." A systematic review of associations between social network site use and romantic relationships. *Computers in Human Behavior*, *75*, 684-703. https://www.doi.org/10.1016/j.chb.2017.06.004

Serrano-Tellería, A. (2018). Users' management of mobile devices and privacy [Cómo gestionan los usuarios sus dispositivos móviles y su privacidad]. *El profesional de la información*, *27*(4), 822-829. https://www.doi.org/10.3145/epi.2018.jul.11

Sheldon, P. & Bryant, K. (2016). Instagram: Motives for its use and relationship to narcissism and contextual age. *Computers in Human Behavior*, *58*, 89-97. https://www.doi.org/10.1016/j.chb.2015.12.059

Shelton, A. K. & Skalski, P. (2014). Blinded by the light: Illuminating the dark side of social network use through content analysis. *Computers in Human Behavior*, *33*, 339-348. https://www.doi.org/10.1016/j.chb.2013.08.017

Steinfield C., Ellison N. B. & Lampe C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology*, *29*(6), 434-445. https://www.doi.org/10.1016/j.appdev.2008.07.002

Tello, L. (2013). Intimacy and "extimacy" in social networks. Ethical boundaries of Facebook [Intimidad y "extimidad" en las redes sociales. Las demarcaciones éticas de Facebook]. *Comunicar*, *41*(XXI), 205-213. https://www.doi.org/10.3916/C41-2013-20

Tokunaga, R. S. (2011). Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. *Computers in Human Behavior*, *27*, 705-713. https://www.doi.org/10.1016/j.chb.2010.08.014

Tokunaga, R. S. (2016). Interpersonal surveillance over social network sites: Applying a theory of negative relational maintenance and the investment model. *Journal of Social and Personal Relationships*, *33*(2), 171-190. https://www.doi.org/0.1177/0265407514568749

Tong, S. T. (2013). Facebook use during relationship termination: Uncertainty reduction and surveillance. *Cyberpsychology, Behavior, and Social Networking*, *16*(11), 788-793. https://www.doi.org/10.1089/cyber.2012.0549

Trottier, D. (2012). Interpersonal surveillance on social media. *Canadian Journal of Communication*, *37*(2), 319-332. https://www.doi.org/10.22230/cjc.2012v37n2a2536

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197-208. https://www.doi.org/10.24908/ss.v12i2.4776

Wang, K., Zhou, M. & Zhang, Z. (2017). Can insecurely attached dating couples get compensated on social network sites? The effect of surveillance. *Computers in Human Behavior*, *73*, 303-310. https://www.doi.org/10.1016/j.chb.2017.03.046

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology,* 30, 75-89. https://www.doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. London: Profile Books Ltf.

ISSN 2386-7876 – © 2020 Communication & Society, 33(1), 139-152