Unpacking (the) Secret: Anonymous social media and the impossibility of networked anonymity

Tzlil Sharon, tzlil.sharon@mail.huji.ac.il
Nicholas John, n.john@huji.ac.il
The Department of Communication, The Hebrew University of Jerusalem, Israel

Introduction

The last few years have seen a flurry of apps for anonymous communication, with Secret, Whisper, Yik Yak, and others attracting millions of users worldwide. Despite differences in their functionality, all of these apps extend the same invitation: speak freely and honestly. Enveloped in this invitation are long-running debates about the ideal conditions for authentic self-expression and the consequences of online anonymity. However, while a great deal has been written about the opportunities and challenges of anonymity in the early days of the internet, we still know very little about the recent wave of anonymous social media, which operate within a new online context. The shift to the real-name web (Hogan, 2013) and the rise of social media call for a reappraisal of how anonymity is perceived and experienced, particularly in one of its newest forms: anonymous communication with friends on tie-based anonymous applications.

In this article we focus on Secret, a mobile application for anonymous communication that operated between 2014-2015, with approximately 15.5 million users at its peak.[1] Secret enabled users to anonymously share messages ('secrets') with their Facebook friends and/or phone contacts. These secrets appeared in a stream, but without user profiles or friends lists. At no point did the application let its users know who had posted or commented on what; it only revealed that a secret had been posted by a 'friend' or a 'friend of friend' (see Figures 1 and 2). Secret thus offered a new social structure that we term *networked anonymity*.[2] As we shall demonstrate, this

term accounts for both the appeal of applications such as Secret, and their inherent instability: people are drawn in because they are given the opportunity to be anonymous among friends; at the same time, the knowledge of connectivity invites constant de-anonymization. Put differently, the very feature that makes networked anonymity so appealing as a model of communication also brings about its collapse. Like chemical elements that can only survive for a number of milliseconds, networked anonymity starts to decay the moment it is brought into the world. We argue that the rise and fall of Secret, and other apps for anonymous communication, are at least partly explained by the model of networked anonymity.

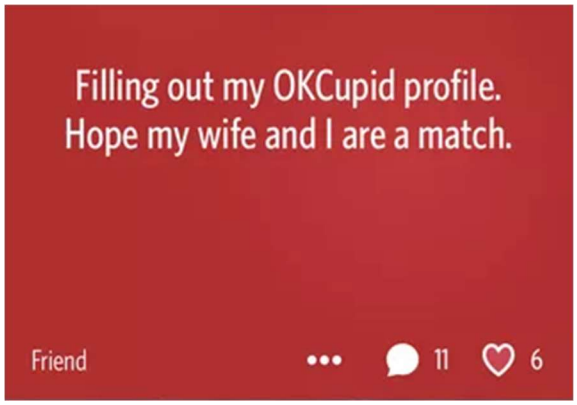

Figure 1: A secret posted by a 'friend' (https://www.theverge.com/2014/2/17/5419834/secret-app-screenshots#2)

Figure 2: A secret posted by a 'friend of friend' (https://www.windowscentral.com/secret-client-6cret-now-available-windows-phone-rudy-huyn)

Background

Anonymity is fundamentally connected to communication, as it makes no sense to conceal one's name if there is no one from whom to conceal it (Marx, 1999). Necessarily rooted in interaction, anonymity is therefore of particular interest to media scholars. Anonymity became an especially fertile ground for research with the opening up of the internet in the mid-1990s. Mediated by the internet, with its text-based conversation rooms and discussion boards without strict identification policies, online anonymity became a widely available form of communication. It was not without controversy, though. For instance, it was argued that anonymous communication leads to deception (Donath, 1998), a lack of accountability (Papacharissi, 2002), and anti-social behaviors such as flaming, trolling and cyberbullying (Moore et al., 2012; Rains, 2007).

Constructive aspects of online anonymity were brought to prominence by Sherry Turkle (1995). She observed that the paucity of identity cues in multi-user dungeons (MUDs) enabled players to explore aspects of their identity that might otherwise have been repressed or ignored. While players were not required to identify themselves to the system, they usually chose a pseudonym through which they could be identified by others. Thus, the impression of anonymity was sustained, while also providing a sense of communal cohesiveness. Indeed, subsequent research showed that certain identity knowledge is essential in order to establish reputation and friendships in online communication services (Donath,1998; Henderson and Gilding 2004; Kennedy, 2006), even in anonymous communities that eschew registration policies as a matter of principle (Bernstein et al., 2011).

Meanwhile, around the turn of the millennium, the distinction between 'anonymous' and 'identifiable', a dichotomy held by early internet researchers, began to dissolve. New definitions

such as 'unreachability' (Nissenbaum, 1999) and 'noncoordinatability of traits' (Wallace, 1999) expanded the scholarly vocabulary for the conceptualization of anonymity in the digital age.

Significantly, though, this body of works relates to an earlier era of the internet. However, over the last 15 years or so, computer-mediated interactions have changed in ways that the literature on anonymity has sometimes struggled to keep up with. The early platforms for anonymous communication have been displaced by social network sites (SNSs) and their real-name policies (Hogan, 2013). While earlier internet tools enabled individuals to constitute private lists of contacts, SNSs allowed users to curate and display those connections (Ellison & boyd, 2013). Today, these connections are made between 'uniquely identifiable profiles', whereas previously, they were seen as linking between 'public or semi-public profiles' (boyd and Ellison, 2007). Identifiability is a key attribute here, because although initially designed to create *new* social ties on the basis of shared interests, SNSs actually gained their popularity by providing users a platform to maintain already existing ties; they drew their strength from the acknowledgment that people want to connect with those they already know, or might know, rather than with complete strangers (boyd, 2014). At the same time, the practice of sharing – including of identity cues – has become the mainstream, as connectivity is seen not only as a technical convenience but a central value (Author 2, 2016; Van Dijck, 2013).

This is not to say that anonymity has been pushed aside altogether. Acknowledging the constructive role of anonymity in self-disclosure, blog services typically offer users the option to be totally anonymous, pseudonymous or identifiable (Qian and Scott, 2007), and SNSs sometimes provide affordances for anonymous communication 'bubbles' within a profile-based system, such as Facebook confession boards (Birnholtz, Merola and Paul, 2015). Furthermore, anonymous communication still prevails in certain areas of the internet, in part for the same reasons it was

celebrated in the 1990s; 4chan and Reddit are the most notable examples. Nevertheless, according to Van Der Nagel (2017) the common use of pseudonyms in those sites can be understood as a practice of deliberately compartmentalizing identities and audiences, for example in the subreddit r/gonewild, where participants adopt pseudonyms in order 'to be seen while keeping safe' (Van Der Nagel and Frith, 2015). While the literature has certainly moved beyond the dichotomy of anonymous/identifiable since the rise of social media, the notion of online anonymity – not as an additional feature or possibility, but as the driving force of many new social apps – is now experienced in a new context that requires further examination.

New models of online anonymity

Ma et al. (2017) distinguish between two hybrid models of anonymity: proximity-based and tie-based. The former includes services that rely on geographical proximity (ascertained through the GPS on one's smartphone), such as Whisper and (the defunct) Yik Yak. In this model, users post statuses that are delivered to other users within a defined proximity. The latter model is based on pre-existing digital ties between users, drawn from SNS or mobile phone contacts, and can be seen in apps like Secret, Mimi (a Chinese app that is very similar to Secret) and, most recently, Sarahah. Here, messages are delivered to users who are already in one's social networks. As such, and as we shall show, users are potentially reachable by and identifiable to one another.

Kang et al. (2016) found that people use anonymous social media to gain social validation from an anonymous crowd despite the lack of cohesive and persistent identifiers, similarly to earlier online pseudonymous communities. They also report that participants feel these apps allow for greater honesty, openness, and diversity of opinion. However, although their study focused on apps that offer different models of anonymity – two proximity-based (Whisper, Yik Yak) and one

tie-based (Secret) – it did not address the different experiences that each of these apps offers their users, and the way that the types of relationship between users shapes the anonymous interaction. There have been several attempts to typify the proximity-based model. Focusing on Whisper, researchers found that it exhibits weak and ephemeral ties, while the possibility for developing strong relationships is strongly influenced by geographic density and frequency of use (Wang, et al., 2014). Additionally, posts were found to exhibit different degrees of anonymity, with some users comfortable at having their identities associated with the message (Correa, et al., 2015). These observations suggest that although proximity-based anonymity is new, the way people interact through these services may not be. Geographical proximity does not seem to change the general impression of strangeness between users, and identity cues trade-offs still appear to serve as a mechanism compensating for the impersonal nature of the anonymous environment, similarly to the dynamic found in anonymous interest-based forums. Moreover, researchers' approaches to anonymity in these new proximity-based apps remain limited to concerns such as moral threats and cyberbullying (see Black, Mezzina and Thompson, 2016; Silva et al., 2016)

Accordingly, it is tie-based anonymity that requires theoretical consideration. While anonymous apps that rely on location as the only anchor for sociability are still likely to create the impression of a room full of strangers, anonymous tie-based apps give the feeling of a room full of friends, but where everybody is blindfolded. What is new about this model is that anonymous interactions revolve around pre-existing digital connections which are publicly displayed and traversable in the SNSs upon which these anonymous services are built. Tie-based anonymous apps can thus be seen as social network sites that have been stripped of their public qualities.

Indeed, we argue that tie-based anonymity should be examined from the perspective of the *network*, given that this is what sets it apart from previous models of anonymity. Tie-based

anonymity exhibits an inherent tension between strangeness and familiarity, or, to borrow from Scannell (2000), between anonymous 'anyones' and identifiable 'someones' (participants who are already socially connected to me). Hence, we ask: What perceptions and practices does the structure of a social network bring to the experience of anonymous communication? How did the knowledge of pre-existing connections between anonymous users shape their expectations from and participation in Secret? What was appealing about this model of anonymity, and what (if anything) does it have to do with the app's downfall? Answering these questions will help to bring the literature on anonymous computer-mediated communication up to date, and will situate the recent wave of apps for anonymous communication in the wider context of social media.

Method

This article is based on twenty semi-structured in-depth interviews with Israeli users of Secret (12 men, eight women) aged 23–46 (average: 29). It was guided by the principles of grounded theory (Strauss & Corbin, 1998), in which analysis and conceptual theorizing progressed from the outset of the research process and in parallel with it. We found the interpretive nature of this approach best suited for investigating the complex uses, attitudes and perceptions regarding the new and under-researched model of anonymity offered by Secret.

Participants were recruited through a Facebook post calling on adult Israelis who had used the app for at least two weeks, following by snowball sampling. Interviews were conducted between May and June 2015, shortly after Secret had announced its sudden shutdown. However, the key period of use mentioned by most interviewees was July-August 2014, which was before Secret changed from a tie-based platform to a proximity- *and* tie-based one. In addition, it should be noted that the sampled population was mainly composed of early adopters in their 20s who study or work in the fields of media and technology, and live in central cities in Israel (Tel Aviv and Jerusalem). While

quite homogenous, the sample fits well with the audience that warmly embraced the app when it was first released in Silicon Valley in the beginning of 2014.

The interviews followed a semi-structured questionnaire with the goal of facilitating a natural conversation-driven dialogue. Users were asked about their perceptions of anonymous communication, focusing on issues of self-presentation, self-disclosure and social dynamics on Secret, in comparison to their uses of and attitudes towards real-name social media. Interviews were conducted face-to-face (except for two that were carried out via Skype), and lasted 60-90 minutes.

The transcribed interviews were imported into software for qualitative data analysis. Coding proceeded in three stages: open, axial and selective coding (Pandit, 1996; Strauss & Corbin, 1998). First, open coding was applied to identify prominent themes across all interviews and fracturing the raw data into 'bricks' of concepts and motifs. Second, axial coding was performed to explore the connections between those bricks, and their relations to anonymity-related themes found in previous studies on anonymous and pseudonymous internet communities, such as disinhibited behaviors, intimacy and support. This stage of analysis was used to define the main categories and their sub-categories (for example, 'fear', 'deception', and 'loneliness' were conjoined to a subcategory of 'negative attitudes towards anonymity', which was subordinated to a higher category of 'users' expectations'). After this integration of categories, the data were reevaluated and a core category was identified: social media-based de-anonymization strategies. This included actions interviewees took to reconstruct the identities of other users on Secret in ways that were specifically related to the network structure of the application. Once the core category was established, we applied a more intense form of coding to typify the different sources, orientations and contexts used to perform each of these de-anonymization practices. This process was carried

out in the selective coding stage (Pandit, 1996), in which an initial theoretical framework was developed to account for the new ways anonymity is perceived and experienced in the context of tie-based anonymity.

Findings

Perceptions

Secret as Facebook's id

The founders of Secret invited users 'to be themselves and share anything they're thinking and feeling with their friends without judgment'.[3] However, this was not why the interviewees came to Secret. In fact, anonymous communication was generally viewed in negative terms, such as 'scary', 'dangerous' and 'faceless', and was often associated with earlier iterations of privacy concerns and the internet. Some interviewees were simply uninterested. For example, Rubi said: 'I must say anonymity is not really all that interesting to me [...] when it comes to anonymous people I'm like, well, I don't really care about their opinions'. Peter went further, stressing that 'I want to be famous and recognized, so anonymity is exactly the opposite of who I am; it's for psychopaths'. Others felt that the contemporary social media environment makes the concept of anonymity redundant. As Bobby said, 'Anonymity is a bit of unicorn nowadays'.

So why *did* they start using Secret? The two most common explanations were boredom ('I was sitting on the toilet and my Facebook feed was running out', said Nikolai) and entertainment-seeking. Additionally, interviewees hoped to read things 'people don't say on Facebook', as Ruby put it, or as Neil said: 'To understand what's really going on in people's heads and not what gets through the filter, because when I'm on Facebook I always filter what I say and what I'm feeling'. At the same time, interviewees did not expect that their friends would be sharing deep secrets, and they themselves had no intention of posting anything that could potentially embarrass them.

Once they had started using Secret, however, the anonymity it offered was significant to the interviewees' identity management and social interactions on the app. To understand this, we should first consider a crucial observation: all interviewees talked about Secret as a social network that was constantly in the shadow of Facebook as a point of reference. This should not come as a surprise, as Secret was technically and conceptually dependent on Facebook, and as mentioned above, Secret reproduced Facebook ties. Nevertheless, it was fundamentally different from Facebook both in display and in function: it had no profiles or friend lists and it did not show connections between friends for others to traverse. However, users still expected it to behave both like Facebook *and* as an antithesis to Facebook, rather than comparing it with other anonymous apps, as this quote from Jasmine implies: 'Facebook is your image. […] Some things you just can't write on Facebook, that's what Secret is for. It is made particularly to [let you] post those things you're too embarrassed to write on Facebook.'

This was also indicated by Anastasia, who claimed that Secret allowed her to enjoy the social benefits and validation she gets from Facebook, but in a more honest way:

> On Facebook […] I never know if I get Likes because I wrote something brilliant […] or because I'm Anastasia, and it's the norm to tell me that I'm an amazing writer. On Secret it's a much greater compliment because people don't know who I am.

Even in terms of terminology, only a few interviewees referred to what they shared or read on Secret as 'secrets'; the more common expressions were 'posts' and 'statuses', the terminology of Facebook. At the same time, being anonymous on Secret led them to self-disclose more than on Facebook, sometimes to the extent of jeopardizing their anonymity. Those self-disclosures were also framed in relation to Facebook, as demonstrated by Rose: 'On Facebook people are always

talking about how great things are and on Secret it's like all the negative stuff, like, the least positive things in people's lives'.

Since Facebook overshadowed the experience of using Secret, going incognito on Secret not only felt liberating, but also seemed to compensate for what had been lost on Facebook: a sense of genuine caring between people one sees as 'friends'. This was described by Greg, with a certain ambiguity, as 'an entire community of people who don't know you, or maybe they do know you, but you don't know that they know you'. Specifically, he spoke of a time when this community offered support to a suicidal user: 'I saw comments like, "man, you are a friend of mine […] talk to me"'. While intimacy between anonymous strangers is a well-known phenomenon (Rubin, 1975; Suler, 2004), almost half of the interviewees connected their willingness to open up to the reassuring knowledge that they were surrounded by friends. Aligned with recent findings on anonymous social media showing that users are more comfortable disclosing to social ties than to people nearby (Ma, Hancock and Naaman, 2016), we see that tie-based anonymity produces a new kind of intimacy between anonymous individuals in a network, in which empathy and openness are enabled specifically by social closeness. As Zion said regarding his recent break-up, on Secret he felt he could 'open up the subject with *friends*, in a more anonymous and discreet format'.

It should be noted, however, that the experience of being anonymous on Secret was also associated by some interviewees with previously reported themes regarding online anonymity. For example, some mentioned the desirable shift away from profiles (Bernstein et al., 2011; Henderson & Gilding, 2004), as Secret gave them 'the opportunity to simply say it, regardless of your gender or identity' (Ophelia). For Greg, a spokesman for public institutions, Secret was stage on which he could express the full complexity of his views without risking his job: 'I was able to be completely critical […] to engage in political discussions without holding myself back'. His words echo the

established ties between anonymous communication and political expression (Coleman, 2011). In addition, two interviewees demonstrated a playful and exploratory use of the mask of anonymity in a similar fashion to that of MUD players in the early days of the internet (Turkle 1995), by signing each post they shared on Secret with a consistent pseudonym.

These findings support what we already know about anonymity, but also tell us something new. Situated in the shadow of Facebook, we learn that Secret was experienced both as a social network *and* as a dissociated anonymous sphere, akin to earlier models of anonymous CMC services, such as IRC and ad-hoc discussion boards. This is exemplified in Bobby's statement that 'on Secret you don't know who's reading it, well, as a matter of fact you do, but somewhere you kind of don't care'. The intriguing tension between familiarity and strangeness described in this excerpt appeared to have a unique effect on how interviewees imagined their anonymous audience on Secret, a point to which we now turn.

The reconstructed imagined audience

The experience of communicating anonymously with friends is not new. Indeed, David Byttow, co-founder of Secret, said that 'Secret feels like a masquerade ball: you know who's on the guest list, but you don't know who is saying what.'[4] Similarly, we can think of Valentine's Day cards, or the game of Secret Santa. With Secret we also have a network comprised of anonymous members with whom we share some kind of social tie, but unlike the previous examples, on Secret participants are also given certain knowledge about those ties. This feature contributes to what Scott (2004) defined as 'source knowledge' – the degree of familiarity between the source and receiver in anonymous communication – as opposed to 'source specification', which concerns the extent to which a message source is distinguished from other possible sources (p. 129). In earlier work of his, Scott argues that these two dimensions shape the concept of anonymity and affect the

likelihood that a receiver will engage in identification efforts, a point on which we elaborate later (Anonymous, 1998).

Seeing that a secret was posted by a 'friend' or a 'friend of friend' obviously creates a general sense of assumed familiarity between anonymous users. But the interviews suggest that the presence of 'friends of friends' creates the possibly misguided impression that we are closely connected to our 'friends'. The distinction between friends and friends of friends meant that each secret could be attributed to distinct sets of people, one of which ('friends') is inherently more interesting than the other. For example, Eric said: 'With "friend of friend" I don't care much beyond the basic voyeurism, but with a "friend" it's something more [meaningful]'. Neil explained that seeing secrets from 'friends' is more appealing because it heightens the drive to de-anonymize:

> Once it's a friend of mine, and once it's a friend of another friend, then it really narrows it down, like the amount of people who could have written that [secret]. Then the attempts begin, it doesn't even matter [who it might be] but it's interesting… the idea of trying to figure out who said what [….] added a game-like aspect.

We already know that audiences on SNSs are imagined (Litt and Hargittai, 2016), and that SNS users imagine the audience that helps them make sense of various social media metrics (Bernstein et al., 2013). On Secret, which was not a social network site but was experienced as such, users felt they were interacting with what we term a *reconstructed imagined audience*, from which individuals who might make us feel uncomfortable are mentally excluded. Interviewees assumed that their anonymous network on Secret was comprised either of people they consider close friends, or people they do not really care about. Interestingly, this imagined network did not include ties that on other platforms might make users feel awkward, such as parents and former bosses. As such, Secret was seen as immune from context collapse (2014). Lily described it as follows: 'On

Facebook it's like you are super-exposed, […] your mother, your Auntie Raya, your cousins […], my boss from five years ago – they are all friends of mine on Facebook. But on Secret it's like the opposite'.

This feeling created the illusion that 'there are no mothers on Secret', as Jasmine put it (although one interviewee was a mother who joined Secret to spy on her teenage daughter). That is to say, the imagined audience on Secret was characterized more by those who were *not* included in it than by those who *were,* and therefore was experienced as a reconstructed and selectively sorted Facebook audience. This false sense of control over the contexts of the imagined audience (previously reported by Bernstein et al., 2013) seems to have taken at least some of the pressure off the interviewees' carefully managed self-presentation on Facebook.

However, after Secret launched its geofenced feed in December 2014, a feature that restricted secrets to people within a certain geographical location, the reassuring promise of being anonymous with friends lost its resonance. The transformation from a tie-based to a proximity-based model created a different setting for anonymous communication, which also led to a change in the perception of the audience in a way that undermined interviewees' motivations for using the app. Josephine, for instance, eventually quit Secret because she felt she was losing that appealing sense of control over her imagined audience: 'the fact that I couldn't choose who to filter meant that kids took over my Secret feed […] I'm not interested in ninth graders, they are not my real circle of friends'.

The anonymity offered by Secret was only appealing for as long as the interviewees felt they were communicating with people whom they could potentially de-anonymize, which was strongly affected by the degree of source knowledge. On the one hand, the absence of unique identifiers, such as names and other profile details, helped them imagine a reconstructed social media

audience, without having to navigate colliding contexts; on the other hand, once this audience became radically anonymous, to the point where they could not de-anonymize it at all, Secret stopped being interesting.

Practices

De-anonymization strategies

The most prevalent practice among the interviewees was de-anonymization. Since the nature of their connection with anonymous sharers was visible to them – 'friend' or 'friend of friend' – the interviewees could draw on this assumed familiarity as a basis on which to reconstruct identities on Secret. A similar finding has been reported by Ma et al. (2017) regarding users of Secret and Mimi, where two types of de-anonymization strategies were identified: 'soft-hacking' (guessing, based on previous knowledge about friends, language and speech cues, etc.) and 'hard-hacking' (such as breaking into Secret's database). However, Ma et al. do not explain how users tried to de-anonymize others, and nor do they explain the significance of de-anonymization to the experience of using Secret. Accordingly, we present four strategies for de-anonymization described by the interviewees, before showing how they are central to the very experience of using Secret, and, we suggest, other apps for tie-based anonymous communication.

(a) Educated guesswork

The first strategy, that of *educated guesswork*, is not exclusive to Secret. It builds on personal interpretations of information that can be extracted from the anonymous message, which is then linked to one's knowledge about one's friends. In some cases, interviewees guessed who had posted secrets based on writing style or a unique turn of phrase that reminded them of a specific friend. For instance, one interviewee believed his best friend recognized a very personal secret of his based on an idiosyncratic turn of phrase. Other interviewees relied on familiar references

provided in the secret. For example, Peter came across a secret that included the name of his friend's employer, and Bobby saw a coming-out-of-the-closet disclosure which he immediately attributed to a friend of his who had recently come out.

(b) Crowdsourced educated guesswork

The second strategy, *crowdsourced educated guesswork*, is similar to the first, though it involves more people. David described this strategy as follows:

> In my friends group on WhatsApp someone would send a screenshot [of a secret he saw on Secret] and there was this whole thing of trying to guess if that's someone we knew. Usually someone would drop a speculation and others would say 'yes' or 'no'.

In other words, not only did users try to link pieces of information from anonymous secrets with extraneous knowledge, as described above, they also sought to verify their educated guesses with mutual friends on other digital platforms.

(c) Cross-referencing with other platforms

This strategy is qualitatively different from the previous two in that it involves another source(s) of information and requires a specific orientation that we can only find in a highly-networked environment. It involves the monitoring of activity of anonymous friends on Secret *and* on other social networks over a parallel timeframe. For example, David remembered seeing on Secret a disturbing confession of infidelity, which he believed had been published by a specific friend of his, and which included the sharer's age. At a later date he saw a comment, which he suspected had been written by the same person (based on their writing style). Because comments to secrets are posted in real time (unlike the secrets themselves, itself an anonymity-protecting feature), David was able to log on to Facebook and see that the person he suspected of writing the comment, and the confession of infidelity, was online. As he explained:

> There was this one time [...] that I recognized a comment of hers. Because I knew her age, I checked who on my Facebook friends list was active at that time, and she was the only friend of that age who was active.

One of the things that stands out about this example is David's computer-like analysis. Re-identifying individuals by linking data from distinct networks, or by analyzing patterns of a person's digital activity, is far from trivial. It requires both a technological orientation and the ability to conceive of identity in terms of digital footprints.

(d) Retrieving the network

The fourth and most complex strategy draws on cross-referencing other social media platforms, while also drawing on other actors in one's network, and in particular their network relations with one another. This was already hinted at in an abovementioned quote from Neil ('Once it's a friend of mine, and once it's a friend of another friend, then it really narrows it down'). Jasmine, however, goes into great detail. In interview, she mentioned having come across a secret, published by a 'friend', that she felt was addressed to her. The secret included a line from one of her boyfriend's favorite songs. Since she and her boyfriend, Mark, were on a break, she interpreted it as his way of letting her know that he missed her. However, Jasmine was not entirely sure, so she set about de-anonymizing the secret:

> I thought to myself, OK, how do I figure this out? I need to find mutual friends who we don't have a lot of mutual friends with, so I asked my brother and sister. [My sister] and Mark don't have many friends in common, and Mark and [my brother] don't have many friends in common. So if they can both see [the secret], and if they see it on their [Secret] feed and it's from 'friend' and not 'friend of friend' then I'd know that that person is my friend, my brother's friend, and my sister's friend, so most likely, then, that it's Mark. I

> mean, who else could it possibly be? So that's what I did. I also asked my brother's girlfriend to look at her Secret feed [...] And it said 'friend' for everyone. Mark is friends with all of them on Facebook, and he's also my friend, so it's Mark. Every time I saw a [secret] like that [...] I just texted them, sent them a screenshot, 'Can you see it on your feed? Does it say "friend"?', and when they said yes, it was like, 'Wow! That's Mark!'

Jasmine's de-anonymization process is multi-layered. Having read a post on Secret, she starts with personal knowledge about the person she suspects of writing it (Mark, her boyfriend), namely, his favorite songs. She does not jump to conclusions, however. Rather, she stops and asks herself, 'how do I figure this out?'. Her technique draws on her ability to visualize her ties with Mark and other mutual contacts as an egocentric network, while at the same time observing the network from the perspective of another node in that network. She embarks on a process of elimination by asking herself which people meet the following conditions: (1) they are close enough to me that I can ask them to help me out (text them, send them screenshots); (2) they are Facebook friends with Mark (otherwise they would not see him as a 'friend' on Secret, but rather as a 'friend of friend' by virtue of their mutual Facebook friendship with Jasmine); and (3) we have a minimal number of additional mutual Facebook friends (otherwise, the person they are both seeing on Secret as a 'friend' might not be Mark but another, different mutual Facebook friend).

Of course, it is not by chance that Jasmine decides that her sister, her brother, and his girlfriend are suitable assistants. In fact, it is precisely because she introduced them to Mark; Mark only knows them because he knows Jasmine. Jasmine (correctly) conceives of herself as the node that links Mark and these other people in her network.

This also shows the multiple layers of networks that Jasmine is navigating. One layer consists of Jasmine's offline social network. This is the network at play when Jasmine is thinking about to

whom she can send screenshots. Another layer is her Facebook network: her efforts at de-anonymization only work because Secret reproduces Facebook ties. Moreover, because she knows what certain parts of that network look like, she can internally visualize them. That is, she knows that she, Mark, and her three helpers are all connected to each other on Facebook. The third layer is the network on Secret, where secrets are presented as having been posted by 'friends' or 'friends of friends'. Having recruited assistants who are close to her, and whose proximity to Jasmine is precisely the reason she recruited them, Jasmine imagines different network configurations in order to de-anonymize the Secret network. In other words, Jasmine tries to make the ties on Secret viewable and traversable; she is trying to turn Secret into a social network site, and she is able to do that precisely because Secret was layered on top of Facebook.

The four strategies for de-anonymization described by the interviewees are summarized in Table 1. They are labelled from (a) to (d) to convey the increasing sophistication of the techniques. The anonymous network referred to here is Secret, but these strategies could be deployed vis-a-vis other tie-based anonymous networks too.

Altogether, the first two strategies were mentioned in 33 different instances by 18 interviewees. We group them because we consider this sort of identification effort as having to do mainly with 'source specification' (Scott, 2004). The second two strategies involve information from Secret and other sources in a way that also requires 'source knowledge' (Scott, 2004). This type of strategy, which brings the degree of connection and familiarity between users to bear, was explicitly described by five interviewees in five different instances. This, however, does not include interviewees sharing a screenshot from Secret with friends on WhatsApp, although these incidences may involve connections outside Secret between all parties and thus may overlap the two groups of strategies.

As noted earlier, the research population was mainly comprised of early adopters, who were tech-oriented young adults. These characteristics no doubt impacted on the described practices, especially the more sophisticated ones. While we do not suggest that the ordinary user of Secret would engage in such cross-referencing attempts or multi-sourced de-anonymization efforts, we maintain that precisely these outstanding examples provide valuable and nuanced knowledge that cannot be accessed otherwise.

	My knowledge	**My knowledge & others' knowledge**
Anonymous network	(a) Educated guesswork	(b) Crowdsourced educated guesswork
Anonymous network & other networks	(c) Cross-referencing	(d) Retrieving the network

Table 1: De-anonymization strategies on tie-based anonymous social media

Discussion: On Secret, everyone knows you're someone

Our findings show the need for a new concept to account for and describe the novel kind of anonymous communication enabled by tie-based applications such as Secret. We find that anonymous communication in Secret is quite different from earlier forms of online anonymity. Building on Scott (1998; 2004), we see this difference play out in two main ways: the degree of perceived anonymity; and the sociotechnical arrangements that are likely to prompt de-anonymization efforts.

Because the difference between Secret and earlier forms of online anonymity lies in the networked nature of the ties between users of the app, we call this *networked anonymity*. Networked anonymity is produced when actors' identities are removed from a pre-existing network, while leaving the structure of the network in place and leaving visible the edges' attributes. In other words, the anonymous actors in this network know what type of connection they share with one

another (on Secret, 'friend' or 'friend of friend'). It is distinct from other models of anonymity in terms of its implications for users' perceptions, motivations and practices. Our central argument is that the concept of anonymity from the early days of the internet, when nobody knew you're a dog, does not apply to tie-based anonymous communication. The recent growth in anonymous social media, Secret included, cannot be analyzed using the theoretical tools from the anonymous computer-mediated environment of the mid-1990s, such as MUDs and IRC, or through cases like the anonymous communities of 4chan. Steps have already been made to conceptualize apps such as Secret as tie-based (Ma et al., 2016; 2017). However, we shift the focus from ties to networks, both as a technical basis and as objects-to-think-with about the meaning and experience of anonymous communication on such platforms.

Due to its networked structure, Secret invited users to imagine each anonymous secret's author as 'someone' rather than as an unknown 'anyone'. Accordingly, interviewees often interpreted the secrets they read as directed at them, and not at an anonymous audience. Here we expand on our earlier mention of Scannell (2000), who argued that in order to appeal to many people at once, media must be organized such that anyone and everyone can use and understand them. He suggests that post-industrial mass media manage to do so because they have a *for-anyone-as-someone* communicative structure. As such, they combine the impersonal and useful *for-anyone* nature of mass products with the personally designed *for-someone* model of custom-made products to simultaneously speak to one and to many. Thus, mass media are able to capture both the anonymous audience of the masses and the particular someone watching the news on TV from his living room. As noted by Scannell, 'it seems that the newsreader in the studio is speaking directly to me […] and yet at the same time this experience is shared by countless others' (pp. 10-11).

In order to explain what the network context does to anonymous media, we suggest turning Scannell's argument on its head: with anonymous social media, the issue is less to do with whom is being talked to and much more to do with who is talking, which such apps conceal from us. Nevertheless, because Secret sat on top of Facebook and made visible the nature of the connection between users, users on Secret felt they were not being spoken to by just *anyone*, but rather by a particular *someone* whom they knew. We thus argue that networked-anonymity based services have a *from-someone-as-anyone* communicative structure, which creates constant instability. Ironically, this instability was the most attractive feature of Secret. It enabled users to feel in control of their social network, as they redrew it in their mind by creating mental maps of restored ties and identities, and thereby undermined the very anonymity Secret offered them. This communicative structure gives the model of networked anonymity its force in an age of real-name policies and publicly articulated profiles. It is a model of anonymity that calls for interruption and invites the reconstruction of identities around a networked self.

Conclusion

We found that the anonymity offered by Secret enabled users to disclose more openly than on other social media platforms, to express unconventional opinions, and to experiment with a wider range of aspects of their identity. It also appeared to play a significant role in interviewees' ability to empathize and share feelings with others, and, in some cases, it was experienced as a tool for promoting content over personality. However, while the connection between these properties and anonymous communication has already been delineated in previous studies, we argue that there is something importantly new about the anonymity offered by Secret, namely, its network context. There are two ways in which networks construct this new kind of anonymity: technical, of course,

but also conceptual. Secret was not only based on pre-existing social networks, but also appealed to its users' network orientation, drawing on the network as a structure of thought.

The rise of the real-name web, with its identity-based profiles on SNSs, did not do away with anonymity, but the context in which anonymous services now operate has dramatically changed. While some aspects of anonymity still draw us to engage in such services, such as the ability to play with our identity, our structure of thought regarding online communities is now networked in essence; we imagine social ties in terms of networks. This is especially relevant when trying to understand the social functions of anonymity for users of Secret. From a network perspective, finding that de-anonymization was the most commonly discussed practice among the interviewees is an affirmation of the wider media context.

In this respect, re-identifying an anonymous author who was shown as a 'friend' or a 'friend of friend' was not solely about de-anonymizing that particular user, but should rather be seen as an attempt to reconstruct one's own network. Analysis of the interviewees' de-anonymization strategies reveals the deep assimilation of a network logic, which corresponds to the communicative structure of from-someone-as-anyone. They navigated secrets as if they were landmarks in an imagined network, where each secret implied a link that could lead to another link, with users drawing on multiple networks simultaneously. That is to say, what makes networked anonymity intriguing is the fact that no anonymous actor can be fully immune from the potential consequences of revealing the nature of their ties within and between anonymous and non-anonymous networks. At the same time, the case of Secret demonstrates why the lifetime of instantiations of this model is inherently limited by competing forces – the drive to connectivity on the one hand, and to anonymity on the other.

Epilogue

On April 29, 2015, Secret announced its closure. Our study does not aim to account for the reasons for Secret's demise after only 16 months of activity. Partly this is because apps come and go for numerous reasons that are beyond the scope of this study, but mainly because our focus here is on perceptions of and practices within a mediated anonymous environment in light of technological and cultural changes. Indeed, the rise of social media has profound implications for expectations and uses of anonymous social apps. Our interviewees found a great deal of interest in Secret for as long as they could rely on connectivity clues to reconstruct the identities of the members of their social network. However, solving the puzzle (or thinking that it has been solved) destabilizes the anonymity of the platform. On the other hand, when Secret became proximity-based and started to resemble a chat room, in which a bunch of anonymous 'anyones' gathered to share random messages, users stopped engaging. In other words, networked anonymity cannot hold stable: indicators of connectivity ('friend', 'friend of friend') enable de-anonymization; their removal means that the users are no longer networked. Hence, the concept of networked anonymity helps us understand not only the success and the failure of Secret, but offers a new way of conceptualizing anonymity in the age of real-name social media.

References

Anonymous (1998) To reveal or not to reveal: A theoretical model of anonymous communication. *Communication Theory* 8: 381-407.

Bernstein MS, Bakshy E, Burke M and Karrer B (2013) Quantifying the invisible audience in social networks. In: *Proceedings of the SIGCHI conference on human factors in computing systems*, Paris, France, 27 April–2 May 2013, pp. 21-30. New York: ACM.

Bernstein MS, Monroy-Hernández A, Harry D, Andrè P, Panovich K and Vargas G (2011) 4chan and /b/: An analysis of anonymity and ephemerality in a large online community. In: *Proceeding of the Fifth International AAAI Conference on Weblogs and Social Media,* pp. 50-57.

Birnholtz J, Merola NAR and Paul A (2015) Is it weird to still be a virgin: Anonymous, locally targeted questions on Facebook confession boards. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, AS, 18-23 April 2015, pp. 2613-2622.

Black EW, Mezzina K and Thompson LA (2016) Anonymous social media: Understanding the content and context of Yik Yak. *Computers in Human Behavior* 57: 17–22.

boyd d (2014) *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

boyd d and Ellison NB (2007) Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13(1): 210–230.

Coleman G (2011) Anonymous: From lulz to collective action. In: The New Everyday. Available at: http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed January 2016).

Correa D, Silva LA, Mondal M, Benevenuto F and Gummadi KP (2015) The many shades of anonymity: Characterizing anonymous social media content. In: *Proceedings of the Ninth AAAI International Conference on Web and Social Media,* Oxford, UK, 26–29 May 2015 pp. 71–80. California: AAAI Press.

Donath, JS (1998) Identity and deception in the virtual community. In: Smith MA and Kollock P (eds) *Communities in Cyberspace.* New York: Routledge, pp.29–59.

Ellison NB and boyd d (2013) Sociality through Social Network Sites. In: Dutton WH (ed) *The Oxford Handbook of Internet Studies.* Oxford: Oxford University Press, pp.151–172.

Henderson S and Gilding M (2004) 'I've never clicked this much with anyone in my life': Trust and hyperpersonal communication in online friendships. *New Media & Society* 6(4): 487–506.

Hogan B (2013) Pseudonyms and the rise of the real-name web. In: Hartley J, Burgess J and Bruns A (eds) *A Companion to New Media Dynamics.* Chichester: Blackwell Publishing, pp. 290–308.

Kang R, Dabbish L and Sutton K (2016) Strangers on your phone: Why people use anonymous communication applications. In: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing,* San Francisco, CA, 27 February–2 March 2016, pp. 359–370. New York: ACM.

Kennedy H (2006) Beyond anonymity, or future directions for internet identity research. *New Media & Society* 8(6): 859–876.

Litt E and Hargittai E (2016) The imagined audience on social network sites. *Social Media+ Society* 2(1). DOI: 10.1177/2056305116633482

Ma X, Andalibi N, Barkhuus L and Naaman M (2017) People are either too fake or too real: Opportunities and challenges in tie-based anonymity. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems,* Denver, CO, 6–11 May 2017, pp. 1781-1793). New York: ACM.

Ma X, Hancock J and Naaman M (2016) Anonymity, intimacy and self-disclosure in social media. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* San Jose, CA, 7-12 May 2016, pp. 3857-3869.

Marx GT (1999) What's in a name? Some reflections on the sociology of anonymity. *The Information Society* 15(2): 99–112.

Moore MJ, Nakano T, Enomoto A and Suda T (2012) Anonymity and roles associated with aggressive posts in an online forum. *Computers in Human Behavior* 28(3): 861–867.

Nissenbaum H (1999) The meaning of anonymity in an information age. *The Information Society* 15(2): 141–144.

Pandit NR (1996) The creation of theory: A recent application of the grounded theory method. *The qualitative report* 2(4): 1–15.

Papacharissi Z (2002) The virtual sphere the internet as a public sphere. *New media & society* 4(1): 9–27.

Qian H and Scott CR (2007) Anonymity and Self-Disclosure on Weblogs. *Journal of Computer-Mediated Communication* 12(4):1428-1451.

Rains SA (2007) The impact of anonymity on perceptions of source credibility and influence in computer-mediated group communication. *Communication Research* 34(1): 100–125.

Rubin Z (1975) Disclosing oneself to a stranger: Reciprocity and its limits. *Journal of Experimental Social Psychology* 11(3): 233–260.

Scannell P (2000) For-anyone-as-someone structures. *Media, Culture & Society* 22(1): 5–24.

Scott CR (2004) Benefits and drawbacks of anonymous online communication: Legal challenges and communicative recommendations. *Free speech yearbook* 41(1): 127-141.

Silva LA, Mondal M, Correa D, Benevenuto F and Weber I (2016) Analyzing the targets of hate in online social media. In: *Proceedings of the Tenth International Conference on Web and Social Media,* Cologne, Germany, 17–20 May 2016, pp. 687–690. California: AAAI Press.

Strauss A and Corbin J (1998) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* Thousand Oaks, CA: Sage.

Suler J (2004) The online disinhibition effect. *Cyberpsychology & Behavior* 7(3): 321–326.

Turkle S (1995) *Life on the Screen: Identity in the Age of the Internet*. New York: Simon and Schsuter.

Van Der Nagel E (2017) From usernames to profiles: the development of pseudonymity in Internet communication. *Internet Histories* 1(20): 312-331.

Van Der Nagel E and Frith J (2015) Anonymity, pseudonymity, and the agency of online Identity: Examining the social Practices of r/Gonewild. *First Monday* 20(3). DOI: 10.5210/fm.v20i3.5615

Van Dijck J (2013) *The culture of connectivity: A critical history of social media*. New York: Oxford University Press.

Wallace KA (1999) Anonymity. *Ethics and Information technology* 1(1): 21–31.

Wang G, Wang B, Wang T, Nika A, Zheng H and Zhao BY (2014) Whispers in the dark: Analysis of an anonymous social network. In *Proceedings of the 2014 Conference on Internet Measurement Conference,* Vancouver, Canada, 5–7 November 2014, pp.137–150. New York: ACM.

Notes

[1] Data presented by company co-founder David Byttow at The Next Web Conference in New York, 2015.

[2] The term 'networked anonymity' has been used in passing by a small number of authors (for instance, in Kevin Savetz's 1994 guidebook 'Your Internet Consultant: The FAQs of Life', and by Douglas Rushkoff in his book 'Program or Be Programmed: Ten Commands for a Digital Age' from 2010), though they have used it simply to mean 'online anonymity'.

3 Speak Freely: Introducing *a new way to connect with friends.* (2014, January 30). Retrieved from https://medium.com/secret-den/speak-freely-61a73ed561b4#.iq4pbjcmq.

[4] Cutler, K. *Anonymity's moment: Secret is like Facebook for what you're really thinking*. Retrieved from https://techcrunch.com/2014/02/03/anonymitys-moment-secret-is-like-facebook-for-what-youre-really-thinking/.