

# Shadow Social Networks

## What You Can't See May Be Hurting You

By Elizabeth Charnock  
CEO, Cataphora



---

In almost every company, there are tightly bound groups of people who are connected, through historical accident, shared experiences, philosophy, origin or any number of common attributes. These groups are typically characterized by closed social interactions and large amounts of trusted “within group” communication – if one member hears a rumor or secret, the whole network will likely soon be up to speed – and a deep sense of loyalty and solidarity. Because they often are invisible to the organization as a whole, we at Cataphora refer to them as “shadow social networks.”

In most instances, these shadow networks are harmless. They provide camaraderie among co-workers and loyalty to an organization. However, shadow networks can become problematic when the group’s goals and objectives diverge from that of the organization. Here again, some of these instances can be harmless. When they are not, however, shadow networks can – and have – taken down multibillion dollar, international corporations.

How can you tell whether the shadow networks within your organization are working against you? While most executives find out only after the damage has been done, there are methods and strategies that can be implemented to detect and thwart renegade shadow networks. This report will explore the defining characteristics of shadow social networks, the damage they have inflicted in some high-profile cases and how a combination of computational linguistics and social network analysis can be an effective way to detect and monitor such groups.

### What is a shadow social network?

As described above, a shadow social network is an informal, yet strongly self-identifying, network of people thrown together by circumstance, experience or common characteristic. A “we take care of our own” attitude can be considered the primary operating principle of such groups, although perceptions of what counts as “our own” can vary widely. Different cultures – and different individuals – often assess which similarities are important in strikingly different ways. Sometimes the ties that bind are obvious even to the unobservant – such as shared ethnicity, common beliefs, or a set of behaviors - while others are nearly invisible. Some examples of the latter that Cataphora has encountered in our investigations of corporate fraud include:

- Former fraternity brothers, nearly 20 years after the fact
- Avid collectors of Nazi memorabilia
- Bondage enthusiasts
- People from the same region of a particular European country, who all spoke the same regional dialect among themselves
- People with a non-obvious shared ethnic or linguistic background (e.g. a grandparent spoke Russian)

As well as much more mundane and obvious connections such as alumni from the same school.

## Shadow Social Networks: What You Can't See May Be Hurting You

---

Interestingly, the obviousness of the connection and the strength of the network are usually unrelated, and it is most often the strength of the perceived connection that strongly implies the desire to help or protect “our own.” The fact that, in today’s society, far fewer people spend their entire careers at the same company only serves to intensify loyalty to the group as opposed to the corporation.

For the most part, such groups are generally benign. Indeed, they are usually and rightly considered to be assets – a social glue that helps aid in employee retention, for example. For this reason, proliferation of shadow networks is often encouraged – or at least passively allowed – which strengthens the natural tendency to hire in one’s own image, potentially expanding that network.

### The dark side of shadow networks

There is, however, a potential dark side to such groups: shadow networks can provide a natural cover that obscures potential – and actual – fraudulent behavior. Because most corporate controls and policies are based on the notion of individuals as actors, they are not set up to detect unified groups acting according to a shared self-interest.

Indeed, the purpose of many types of corporate controls is to make sure that any kind of serious fraud would require the active cooperation of as many different people as possible. Such policies are effective controls because each additional person who must be recruited introduces the risk of detection and raises the risk of disagreements and infighting in the group that would lead to the plan being either abandoned or thwarted.

Shadow social networks, however, provide a fairly effective countermeasure to such precautions since, if members of the already trusted network can be enlisted, the risk of breaking ranks decreases significantly. For this reason, many corporate policies prevent family members from holding positions in which such cooperation would be possible. The good news: some fraud is probably prevented this way each year. The bad news: unless the relationship is a hidden one, all things being equal, the probability of attempted theft or fraud by related employees is not very high, because it would be just too obvious.

To take a very simple example, it is quite easy to steal paperclips, if that is one’s ambition. It is very low risk (if very low pay off), it takes only a few seconds and the paperclips are easily hidden inside a pocket or purse. There’s no need to circumvent any kind of security, and no cooperation is required on the part of anyone else. True, the corporation could act to better secure its paperclip supply, but the cost of doing so in time and money simply would not be worthwhile relative to the potential savings.

Once we start talking about something valuable, however, everything changes. For example, multiple signatures from authorities in different departments and/or at different organizational levels are often needed to move non-routine large sums of money around. This way, it takes several people to cheat; no one person can do it by himself. The overhead and cost of the controls are deemed a necessity.

## Shadow Social Networks: What You Can't See May Be Hurting You

---

A shadow social network with members in the right positions can skirt this type of standard control. It becomes easier to cheat because, even if other members don't actively help, they are far less likely to report a questionable or bad action if they can rationalize not doing so. Conversely, if an individual is looking to commit fraud, he or she will often try to recruit accomplices based on some shared attribute.

### Shadow networks and Société Générale

For example, in the 2008 Société Générale case in which a low-ranking 31-year-old trader lost \$7.2 billion in highly risky trades as the market moved south, much was made of the fact that the trader in question was of humble family origins. He did not attend one of the well considered "Grandes Ecoles" whose graduates comprised the major shadow social networks in the bank and who generally held the higher status positions. Many who analyzed the events in the French press suggested that the costly stunt was a desperate move on the part of the ambitious trader to get "in," to cease to be invisible. It was also frequently observed that perhaps the security failure was due to the fact that his better pedigreed superiors simply didn't bother to consider what anyone outside of their network might be doing – at least not until it was far too late.

Despite his undistinguished background, the trader found accomplices; unsurprisingly these were "outsiders" who, like himself, lacked the kind of pedigree that was so highly valued by his employer. Indeed, sometimes the defining and binding characteristic of a shadow social network is the *lack* of an attribute held by others. Further, once the trader started showing such apparent large gains, a new network was formed around him, of those who had an interest for one reason or another in his continued posting of outrageously large results. Such a shadow social network is based on motive, and will likely evaporate once that motive disappears. Such a connection between individuals, once made, however, is likely to reappear in the future should similar circumstances recur.

Sometimes the origin of the shadow social network is as simple as a set of personal relationships that have been continuously fortified over the course of many years, even decades. For example, Annette Bongiorno, Bernie Madoff's personal secretary for some 40 years, rather unusually, had a small staff. The people who worked for her allegedly created fictional stock trade confirmations for client accounts. Noting the unusual staffing arrangement or the very longstanding relationship could have led to a closer examination of what these people were paid to do; that they were creating fictional stock trade confirmations would doubtless have attracted attention.

### Exploiting loopholes via shadow networks

Sometimes, an otherwise innocent shadow social network can be exploited by a single bad apple who leverages the set of trusted relationships to commit fraud. The most common case we see of this are ones in which people with distinctly different sets of knowledge are thrown together to complete a complex task. While one person may be able to perform a basic sanity check of the work of another, there will always be aspects of the work that will be unfamiliar. If there is a trusted relationship at work, one is far likelier to not look too closely at anything that is difficult to interpret correctly. In this way, loopholes to different kinds of fraud may be found. Many

## Shadow Social Networks: What You Can't See May Be Hurting You

---

things to do with international accounting and finance fall into this category, since different countries can have vastly different rules.

Shadow social networks generally start to become problematic whenever the interests of the group and the corporation potentially diverge, and not always in ways that are fraudulent per se. For example, such networks unsurprisingly tend to be less impacted during layoffs, as decision-makers within the shadow network work to protect “one’s own.” Likewise, an otherwise stellar candidate for a job might be bypassed if she were known to have views that were clearly incompatible with those of the group (e.g. a fundamentalist Christian in the context of the bondage enthusiasts).

However, these networks can also become problematic simply because the number of trusted people within the workplace increases the chances of illicit communication being committed to the electronic record, increasing the risk of civil or criminal liability. For example, two former Bear Stearns hedge fund managers were arrested for fraud due to comments shared with trusted colleagues via email over an extended period of time. The comments made within the network were substantially grimmer than those made to prospective investors. While it is certainly part of the job of salespeople to “spin” their wares, the contrast between the spin in this case, and other emails, which candidly discussed personal fears of failure, among these colleagues (who obviously also had close personal ties) clearly crossed some line in the sand.

Thanks to modern communication methods, the presence of such networks can usually be assessed with technology that combines social network analysis and computational linguistics. The key is not just to identify groups of people who frequently communicate in a “within group” fashion, but also to understand whether that communication is routine or unusual, personal or professional, heavily slanted toward special interest topics or general, etc. In other words, the content must be analyzed in order to understand whether the group is one that is merely forced together by the task at hand, or a volitional one; if a volitional one, what is its defining characteristic? The choice of spoken language can also be a factor. Of specific interest are cases in which the people are clearly multi-lingual, but prefer to use a language other than the default one (such as English, for most U.S.-based organizations) to discuss specific topics. Whether the language switch is for privacy, to achieve a higher level of expressiveness, or to conceal some kind of misconduct, it is indicative of a close connection.

































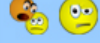



### Determining Patterns of Communication

Clues to the existence of a shadow social network can be derived from a variety of analyses made available by Cataphora technology, which has been used in numerous investigations over the course of more than seven years.

The diagram below shows communication patterns within an organization about a topic that is the subject of an investigation. The left side of the diagram shows a group of ten individuals who communicate very frequently and pretty much only with each other about this topic. This group constitutes a clique. The identifying characteristics of a clique are that the members all communicate with each other to a significant degree and communicate much less, overall, with people outside the clique. These people are probably not all in one department or geographical location, and the bond that ties them together is typically an obscure characteristic.

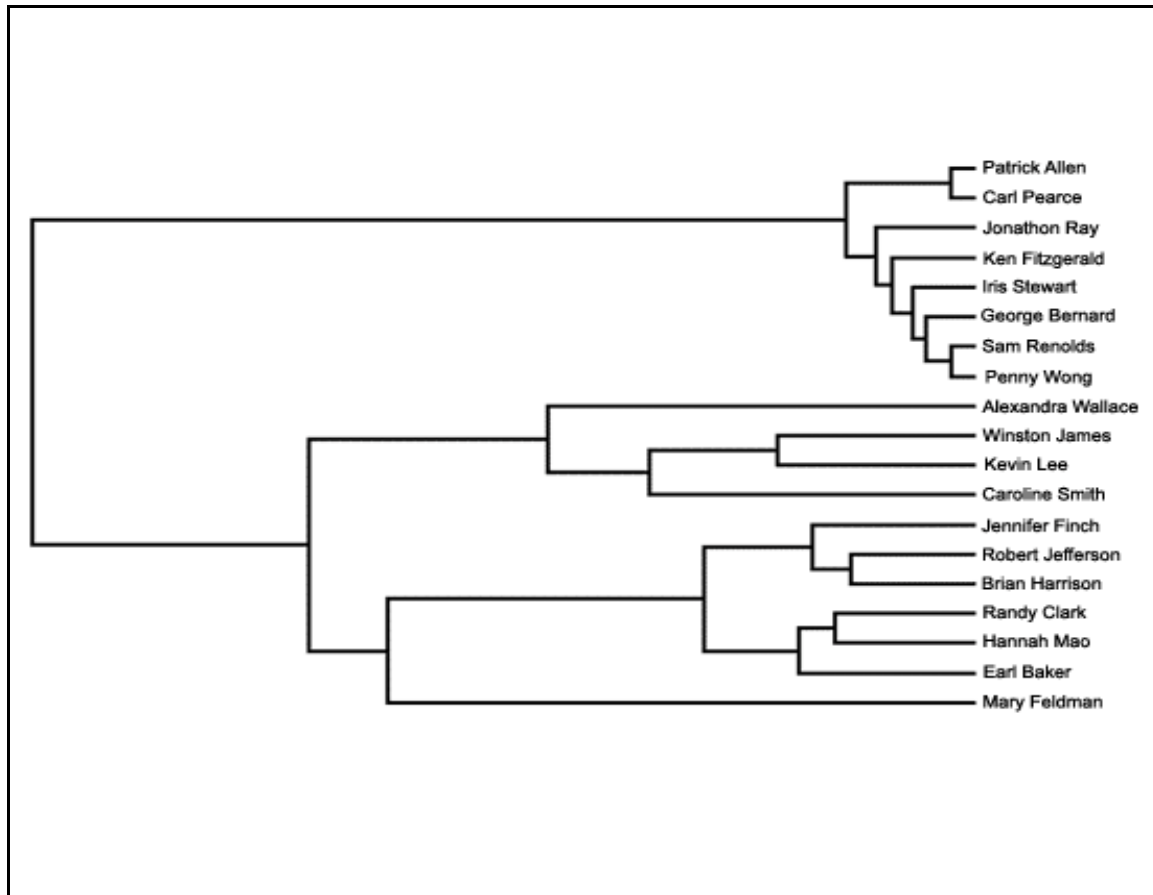


## Shadow Social Networks: What You Can't See May Be Hurting You

	Pierson Merger	3rd Quarter Revenues	Product Launch	Healberg Acquisition	Barcelona Office	New Pension Plan	<b>Tone Analysis</b> 12/01/1999 - 12/31/2001
 Accounting							<ul style="list-style-type: none"> <li> No Content</li> <li> Content With No Tone</li> <li> Tone Present</li> <li> Reverse Sentiments</li> <li> Derogatory</li> <li> Frustrated</li> <li> Secretive</li> <li> Worried</li> <li> Happy</li> <li> Surprised</li> <li> Angry</li> <li> Cursing</li> <li> Problem</li> <li> Confused</li> <li> Suspicious</li> </ul>
 Marketing							
 Reynolds, Cohen...							
 Boston Office							
 San Diego Office							

A further example of an indirect measure shows another situation in which a group of individuals all appear to act in a very distinctly similar way. The diagram below – known as a dendrogram – shows the similarity of deletion patterns for communications around a given topic among various individuals. Horizontal distance indicates similarity. The shorter the horizontal distance (from right to left) before two people's lines are linked (such as is the case for Patrick Allen and Carl Pearce), the more similar their deletion patterns for the data in question. By contrast, a longer horizontal distance (such as that between Winston James and Kevin Lee), indicates a lower degree of similarity.

As is readily apparent, the deletion patterns for the first eight individuals at the top of this diagram are very similar. Did this particular group of people perhaps delete a set of messages or documents shortly before investigators arrived on the scene or a subpoena was issued? While it could be coincidence, it also could indicate that members of a shadow network alerted each other and determined that this course of action was in their best interests.



Another useful analytic, seemingly simple on the surface, examines the number and nature of the contact channels present and used (if this is possible to measure) among pairs of individuals. Channels may include personal and business telephone numbers, instant messaging, personal and business e-mail addresses and text messaging. In general, a larger number of contact channels implies a greater level of familiarity between actors and may imply a closer relationship than might be readily apparent. For example, the presence of several different home addresses for an individual suggests a long period of acquaintanceship. Many different types of contact channels suggest a personal or professional relationship that is close enough to warrant the use of so many different ways to connect to one another.

### What your organization can do

While the depth, size and mere presence of shadow social networks are often not understood prior to a significant scandal or lawsuit, this needn't be the case; software scans and analytics like the ones shown above can identify such groups before any potential business catastrophe. Cataphora takes the point of view that it is exactly this type of scan that should be performed on an ongoing basis, and that the results should be integrated with an organization's compliance monitoring and fraud detection systems. In this way, corporations would have an early warning system of, for example, anomalies in who is handling specific steps in workflow processes that involve large sums of money. A non-routine workflow can spell serious trouble if the people in question are all members of the same shadow social network.

## Shadow Social Networks: What You Can't See May Be Hurting You

---

At Cataphora, our position is that these shadow social networks are neither inherently good nor bad, just as allowing family members to work in the same corporation is neither inherently good nor bad. However, for the exact same reasons that corporations want to know about the family relationships, they should also want to know about shadow social networks. In fact, knowing about the networks is much more important because ignorance of them is much more dangerous, especially if they are submerged and large or well-positioned.