INVESTIGATION · JOURNALISM AND PUBLIC INVESTIGATION

Community Tip Lines and Public Contribution to Investigative Knowledge

Members of the public supply much of the information that solves crimes and uncovers wrongdoing, through tip lines, whistleblowing channels, public appeals and online crowdsourcing. This article examines the evidence on what public information contributes, why people do or do not come forward, how tips should be handled and assessed, the risks of misinformation and online vigilantism, and how organisations can design channels that produce reliable knowledge.

ModQu research article · 2,924 words · 28 references (APA 7th edition)

Investigators rarely discover the facts of a case by themselves. Much of what they learn comes from other people: victims, witnesses, neighbours, colleagues, customers and, increasingly, strangers who notice something online. Police forces run anonymous tip lines and appeal for witnesses. Companies run whistleblowing hotlines. Regulators invite complaints. Journalists ask readers for information. Online communities analyse photographs and videos to identify people and places. Together, these channels make the public one of the most important sources of investigative knowledge.

Public contribution is also one of the most difficult sources to manage. Tips vary enormously in quality, from precise first-hand observations to rumour, speculation and malicious accusation. Large appeals can generate more information than investigators can process. Online crowds can identify suspects in hours, but they can also identify the wrong person and cause lasting harm. This article examines what research shows about the contribution of the public to investigations, why people come forward or stay silent, how tips should be received and assessed, the risks of crowdsourced investigation, and the design of channels that produce reliable knowledge.

How much investigations depend on the public

Research on criminal investigation has consistently found that information from the public is the main reason cases are solved. A major RAND Corporation study of criminal investigation in the United States found that the most important determinant of whether a case was solved was the information provided by the victim or witnesses at the outset; if the identity of a suspect was not known from these sources early on, later detective work rarely produced it (Greenwood et al., 1977). Eck (1983), studying burglary and robbery investigations, similarly found that information from victims, witnesses and other members of the public was central to case solution, although he also showed that follow-up work by detectives could add value in cases with moderate levels of initial information.

Homicide investigation shows the same pattern. Wellford and Cronin (1999), analysing homicide clearance across several United States cities, found that the actions associated with clearing cases included quickly locating and interviewing witnesses and canvassing neighbourhoods for information. Innes (2003), in an ethnographic study of homicide detectives in England, described investigation as the progressive assembly of information, much of it supplied by people in the victim's social world.

The pattern extends beyond crime. In the Association of Certified Fraud Examiners' global study of occupational fraud, tips were by far the most common way frauds were detected, accounting for 43 per cent of cases, more than internal audit and management review combined; more than half of tips came from employees (Association of Certified Fraud Examiners [ACFE], 2024). Dyck et al. (2010), studying major corporate frauds in the United States, found that employees, journalists and industry regulators, rather than auditors or the main securities regulator, were among the most important sources of detection, and argued that monetary incentives for whistleblowers could increase reporting.

Types of public contribution

Public contribution takes several forms, each with different strengths and risks.

Witness reports and appeals. Investigators ask people who saw or know something to come forward, through door-to-door enquiries, posters, media appeals and social media. These reports can provide direct first-hand evidence, but also attract well-meaning but mistaken information.

Anonymous tip lines. Programmes such as Crime Stoppers, which began in the United States in 1976 and spread internationally, allow people to report information anonymously, often with the possibility of a reward. Rosenbaum et al. (1989), in a national evaluation of Crime Stoppers programmes, found that they produced information that helped solve some serious crimes that would otherwise have been difficult to solve, but that the overall number of cases solved was modest relative to total crime, and that results depended heavily on how programmes were run.

Whistleblowing channels. Organisations provide confidential or anonymous channels for employees and others to report misconduct. European Union law now requires many organisations to establish internal reporting channels and protects reporters from retaliation (Directive (EU) 2019/1937, 2019), and an international standard gives guidance on managing whistleblowing systems (International Organization for Standardization [ISO], 2021).

Online crowdsourcing. Howe (2006) coined the term "crowdsourcing" to describe outsourcing tasks to large, undefined groups of people through open calls. Brabham (2013) describes how crowdsourcing can solve problems by drawing on distributed knowledge and effort. In investigation, crowds analyse images, videos and documents, geolocate photographs, identify objects and people, and track events in real time.

Open-source investigation communities. Groups such as Bellingcat have developed rigorous methods for using publicly available information, and often involve volunteers in their work. Higgins (2021) describes how this approach identified those responsible for the downing of Malaysia Airlines Flight MH17. The Berkeley Protocol sets out standards for collecting and verifying such information so that it can be used in legal proceedings (Human Rights Center, University of California, Berkeley, School of Law & United Nations Office of the High Commissioner for Human Rights, 2022).

Channels for public contribution

Each channel produces different kinds of information and carries different risks

	Main strength	Main risk
Witness appeals	First-hand accounts of specific events	Large volumes of mistaken or irrelevant reports
Anonymous tip lines	Information from people afraid to be identified	Cannot ask follow-up questions; malicious tips
Whistleblowing channels	Insider knowledge of misconduct	Reporters fear retaliation; weak follow-up
Online crowdsourcing	Speed and scale of analysis	Misidentification and harm to innocent people
Open-source communities	Rigorous verification of public material	Varying standards; evidence handling for court

ModQu analysis of sources cited in this article ModQu.com

Figure 1. The main channels through which the public contributes to investigations, with the main strength and risk of each. Diagram by ModQu.

Why people come forward, or do not

Whether people share what they know depends on their relationship with the investigating body. Sunshine and Tyler (2003) found that people's willingness to cooperate with the police depended strongly on whether they viewed the police as legitimate, which in turn depended mainly on whether they believed the police acted fairly, rather than on how effective they thought the police were. Tyler and Fagan (2008) found that people who viewed the police as legitimate were more willing to report crimes and to provide information, and that perceptions of procedural fairness shaped legitimacy.

Loss of trust reduces reporting. Desmond et al. (2016) found that after a widely publicised case of police violence against an unarmed Black man in Milwaukee, calls to the police from Black neighbourhoods fell substantially for more than a year. Skogan (2006), studying community policing in Chicago, found that building relationships between police and residents required sustained effort and that participation varied greatly between communities.

In organisations, the same principles apply. Employees report misconduct when they believe their report will be taken seriously, handled fairly and kept confidential, and when they do not fear retaliation. Kaplan and Schultz (2007) found that the availability of an anonymous reporting channel influenced intentions to report, but that it could reduce the use of non-anonymous channels, suggesting that organisations need to offer several routes. Fear of retaliation is the main reason people stay silent; laws protecting whistleblowers aim to address it.

Other factors also matter. People may not realise that what they saw is significant, may not know how to report it, may distrust the specific channel, may fear involvement in legal proceedings, or may have loyalties to the people involved. Appeals that explain exactly what information is wanted, why it matters and how the reporter will be protected tend to be more effective.

Rewards and incentives

Many tip programmes offer rewards. Crime Stoppers programmes typically pay modest cash rewards for information that leads to an arrest, and some regulators pay whistleblowers a share of the penalties recovered. Dyck et al. (2010) found that in industries where whistleblowers could receive substantial financial rewards, such as healthcare fraud under laws allowing private claims on behalf of the government, employees played a larger role in detecting fraud, suggesting that incentives increase reporting. Rosenbaum et al. (1989), however, found that many Crime Stoppers callers did not claim their rewards, indicating that other motives, such as a sense of civic duty or a wish to see a particular offender caught, were often more important than money.

Rewards also create risks. They can attract false or exaggerated reports from people hoping to profit, and they can be used by defence lawyers to challenge the credibility of a witness who was paid. Investigators should record whether a reporter was aware of a reward, assess tips from people seeking payment with particular care, and seek corroboration before relying on them.

Receiving and recording tips

Tip handling begins with reception. Whether a tip arrives by phone, web form, email or social media, the person receiving it should record the information as fully and accurately as possible, in the reporter's own words, together with how the reporter knows it. Was it seen directly, heard from someone else, inferred, or read online? The distinction is essential for later assessment.

Where the channel allows, the receiver should ask open questions to obtain detail, avoid suggesting answers, and ask whether the reporter has told anyone else or seen media coverage. Research on eyewitness memory shows that information from other witnesses or the media can alter what people remember. Gabbert et al. (2003) found that witnesses who discussed an event with another witness often incorporated details the other had seen into their own accounts. Loftus (2005) summarised decades of research showing that misleading information after an event can change memory. A tip that repeats details already published may reflect the media coverage rather than independent knowledge.

Each tip should be logged in a system that assigns it a reference, records the date and time, the channel, the content, the reporter's details or anonymity, and the actions taken. This allows tips to be cross-referenced, prevents duplicate handling, and provides an audit trail if decisions are later questioned.

Assessing tips

Not all tips deserve equal weight. A structured assessment considers several factors:

- **Source.** Is the reporter identified or anonymous? Do they have a known track record? Do they have a motive to mislead, such as a grudge or a reward?
- **Basis of knowledge.** Did the reporter see or hear the information directly, or is it second-hand or speculative?
- **Specificity.** Does the tip contain specific, checkable details, such as names, places, times and descriptions?
- **Consistency.** Does it fit with what is already known, and if not, could it reveal something new?
- **Corroboration.** Can it be confirmed by independent evidence?
- **Independence.** Does it repeat information already in the public domain?

Intelligence services use two-part grading systems that separate the reliability of the source from the credibility of the information, and similar approaches can be applied to tips, provided the categories are clearly defined (Irwin & Mandel, 2019).

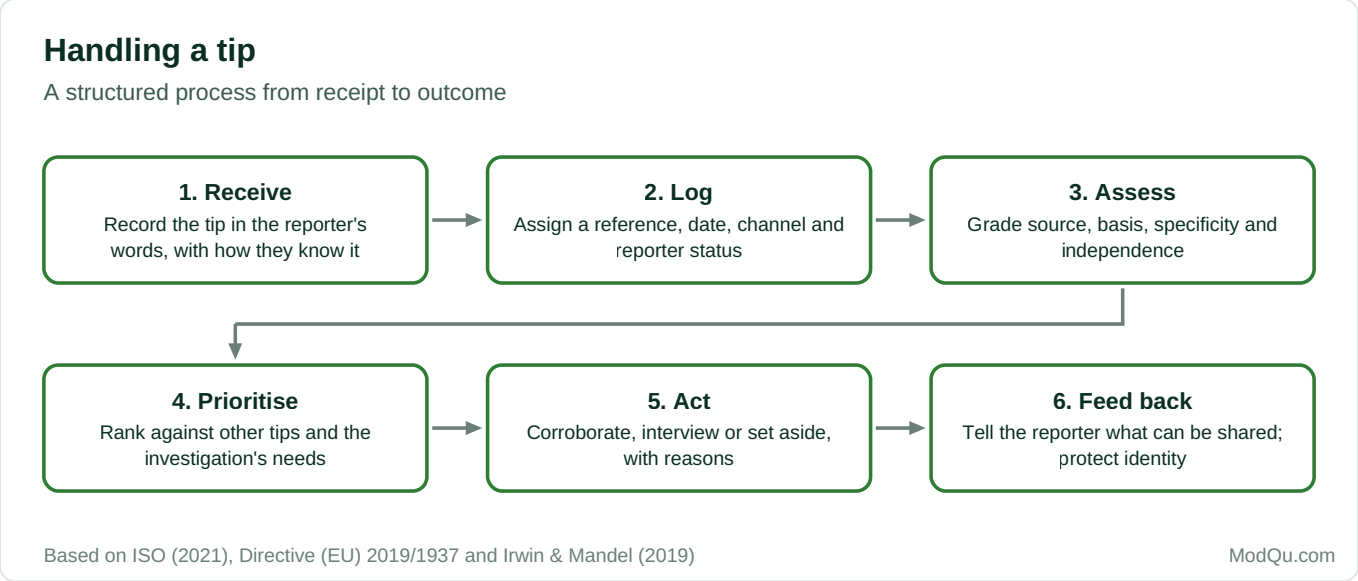


Figure 2. A structured process for handling tips. Recording how the reporter knows the information, and whether it repeats published details, is essential for later assessment. Diagram by ModQu.

When information overwhelms

Large appeals can generate more information than investigators can process, and important tips can be lost among irrelevant ones. The review of the West Yorkshire Police investigation into the "Yorkshire Ripper" murders between 1975 and 1981 found that the investigation's paper-based information system had become overwhelmed by the volume of material, and that the eventual offender had been interviewed several times without the connections between pieces of information being recognised (Byford, 1981). The review led to the development of computerised major incident systems in the United Kingdom.

Rossmo (2009) identifies information overload, alongside cognitive bias and organisational pressures, as a recurring cause of investigative failure. Investigators can manage volume by defining clearly what information they are seeking, using systems that link tips to people, places and events, assigning priorities systematically, and reviewing low-priority tips periodically in case later developments make them significant.

Online crowds and digital vigilantism

Social media allow large numbers of people to take part in investigations directly, without the involvement of investigators. The results can be valuable or damaging.

The response to the Boston Marathon bombing in 2013 illustrates both. Members of the public supplied photographs and videos that helped the FBI identify the suspects. At the same time, users of online forums carried out their own analysis of images and wrongly identified several people as suspects, including a missing student, whose family was harassed. Starbird et al. (2014) analysed the spread of rumours and misinformation on Twitter after the bombing and found that false claims spread widely and that corrections reached far fewer people. Nhan et al. (2017) examined the online communities involved and described "digilantism", in which members of the public assume an investigative role, often with good intentions but limited skills and few safeguards.

Trottier (2017) describes digital vigilantism as the use of online visibility to expose and punish people perceived to have done wrong, often with consequences disproportionate to the alleged conduct and without due process. Huey et al. (2013) examined civilian groups that pursue online offenders, and noted the tensions between their activity and the work of police. Public appeals for missing children illustrate a related problem: Griffin and Miller (2008) argued that AMBER Alert systems, while popular, may produce symbolic reassurance more than measurable improvements in recovering abducted children, and that the alerts generate many false sightings.

These cases show that crowds can contribute observations and analysis, but they lack the controls that make investigations reliable: verification, consideration of alternative explanations, protection of people under suspicion and accountability for errors. Investigators who invite public analysis should be clear about what is wanted, should not release information that encourages speculation about individuals, and should correct false identifications quickly and publicly.

Protecting reporters and the people reported

Tip channels must protect two groups. Reporters need protection from retaliation and, where promised, confidentiality or anonymity. Failure to protect a reporter's identity can expose them to harm and deter future reporting. Whistleblowing laws, such as the European Union directive, prohibit retaliation, require confidentiality and require organisations to acknowledge reports and provide feedback within set periods (Directive (EU) 2019/1937, 2019).

People who are the subject of tips also need protection. A tip is an allegation, not a finding. It may be mistaken or malicious. Investigators should keep tips confidential, avoid acting on unverified tips in ways that harm people's reputations or livelihoods, and give people the opportunity to respond to allegations before conclusions are reached. Data protection law applies to the personal information contained in tips, and organisations should retain tip records only as long as necessary.

Designing effective channels

Research and practice suggest several principles for channels that produce reliable knowledge.

- **Offer several routes.** Provide named, confidential and anonymous options, and more than one medium, because different people prefer different routes.
- **Make reporting easy.** Explain what information is wanted, why, and how it will be handled. Avoid complex forms.
- **Allow two-way contact.** Anonymous channels that allow follow-up questions, for example through a case number and password, produce more useful information than one-way reports.
- **Record how reporters know.** Ask whether information is first-hand, second-hand or inferred, and whether the reporter has seen media coverage.
- **Respond and give feedback.** Acknowledge every report and tell reporters what can be shared about the outcome. Silence discourages future reporting.
- **Build trust.** Fair treatment of reporters and of the people reported builds the legitimacy that makes people willing to come forward in future (Tyler & Fagan, 2008).
- **Measure performance.** Track how many tips are received, how they are assessed, how many contribute to outcomes and how long handling takes, and use the results to improve the channel.

Measuring the value of public information

Organisations often know how many tips they receive but not how many make a difference. Useful measures include the proportion of tips that are first-hand, the proportion corroborated, the proportion that contribute to an outcome, the time taken to assess each tip, and the number of reporters who use the channel again. The occupational fraud data showing that tips are the leading method of detection (ACFE, 2024) suggest that well-run channels repay the investment, but each organisation needs its own evidence. Reviewing a sample of closed tips periodically, including those set aside, can reveal whether assessment criteria are working or whether valuable information is being missed.

A short example

The following hypothetical case shows these principles in practice. A survey research company suspects that some interviewers in one region have been inventing interview responses. It sends a message to all its interviewers and supervisors explaining the concern in general terms, describing what kind of information would help, and offering three routes: a named report to the quality manager, a confidential report to an independent ethics officer, and an anonymous web form with a case number for follow-up.

Fourteen reports arrive. The quality team logs each one and records how the reporter knows what they report. Six are first-hand accounts from supervisors who noticed interviews completed at implausible speeds; four are second-hand reports repeating rumours; three concern unrelated grievances; and one, submitted anonymously, names a specific interviewer and describes a technique for generating responses. Through the case number, the team asks the anonymous reporter follow-up questions, which produce precise details about dates and locations. The team corroborates the first-hand reports and the anonymous tip against interview timestamps, GPS data and callbacks to respondents, confirming

fabrication by two interviewers and clearing a third who had been named in rumours. The company tells reporters, in general terms, that the concerns were investigated and action taken, and reviews its monitoring so that similar patterns are detected sooner.

Conclusion

Members of the public supply much of the information on which investigations depend. Research on crime, fraud and corporate misconduct consistently shows that tips, witness reports and whistleblowing are among the most important sources of investigative knowledge. Whether people come forward depends on whether they trust the investigating body and believe they will be protected. Public information varies greatly in quality, and online crowds can spread misinformation and harm innocent people as easily as they can help. Investigators who design accessible and secure channels, record how reporters know what they report, assess tips systematically, manage volume, protect both reporters and the people reported, and give feedback can turn public contribution into reliable knowledge.

References

Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*.

Brabham, D. C. (2013). *Crowdsourcing*. MIT Press.

Byford, L. (1981). *The Yorkshire Ripper case: Review of the police investigation of the case*. Home Office.

Desmond, M., Papachristos, A. V., & Kirk, D. S. (2016). Police violence and citizen crime reporting in the Black community. *American Sociological Review, 81*(5), 857–876. https://doi.org/10.1177/0003122416663494

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. (2019). *Official Journal of the European Union, L 305*, 17–56.

Dyck, A., Morse, A., & Zingales, L. (2010). Who blows the whistle on corporate fraud? *The Journal of Finance, 65*(6), 2213–2253. https://doi.org/10.1111/j.1540-6261.2010.01614.x

Eck, J. E. (1983). *Solving crimes: The investigation of burglary and robbery*. Police Executive Research Forum.

Gabbert, F., Memon, A., & Allan, K. (2003). Memory conformity: Can eyewitnesses influence each other's memories for an event? *Applied Cognitive Psychology, 17*(5), 533–543. https://doi.org/10.1002/acp.885

Greenwood, P. W., Chaiken, J. M., & Petersilia, J. (1977). *The criminal investigation process*. D. C. Heath.

Griffin, T., & Miller, M. K. (2008). Child abduction, AMBER Alert, and crime control theater. *Criminal Justice Review, 33*(2), 159–176. https://doi.org/10.1177/0734016808316778

Higgins, E. (2021). *We are Bellingcat: An intelligence agency for the people*. Bloomsbury.

Howe, J. (2006). The rise of crowdsourcing. *Wired*, *14*(6).

Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice, 13*(1), 81–97. https://doi.org/10.1177/1748895812448086

Human Rights Center, University of California, Berkeley, School of Law, & United Nations Office of the High Commissioner for Human Rights. (2022). *Berkeley protocol on digital open source investigations: A practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law*. United Nations.

Innes, M. (2003). *Investigating murder: Detective work and the police response to criminal homicide*. Oxford University Press.

International Organization for Standardization. (2021). *Whistleblowing management systems — Guidelines* (ISO Standard No. 37002:2021).

Irwin, D., & Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security, 34*(4), 503–525. https://doi.org/10.1080/02684527.2019.1569343

Kaplan, S. E., & Schultz, J. J. (2007). Intentions to report questionable acts: An examination of the influence of anonymous reporting channel, internal audit quality, and setting. *Journal of Business Ethics, 71*(2), 109–124. https://doi.org/10.1007/s10551-006-0021-6

Loftus, E. F. (2005). Planting misinformation in the human mind: A 30-year investigation of the malleability of memory. *Learning & Memory, 12*(4), 361–366. https://doi.org/10.1101/lm.94705

Nhan, J., Huey, L., & Broll, R. (2017). Digilantism: An analysis of crowdsourcing and the Boston Marathon bombings. *The British Journal of Criminology, 57*(2), 341–361. https://doi.org/10.1093/bjc/azv118

Rosenbaum, D. P., Lurigio, A. J., & Lavrakas, P. J. (1989). Enhancing citizen participation and solving serious crime: A national evaluation of Crime Stoppers programs. *Crime & Delinquency, 35*(3), 401–420. https://doi.org/10.1177/0011128789035003005

Rossmo, D. K. (2009). *Criminal investigative failures*. CRC Press.

Skogan, W. G. (2006). *Police and community in Chicago: A tale of three cities*. Oxford University Press.

Starbird, K., Maddock, J., Orand, M., Achterman, P., & Mason, R. M. (2014). Rumors, false flags, and digital vigilantes: Misinformation on Twitter after the 2013 Boston Marathon bombing. In *iConference 2014 Proceedings* (pp. 654–662). iSchools. https://doi.org/10.9776/14308

Sunshine, J., & Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law & Society Review, 37*(3), 513–548. https://doi.org/10.1111/1540-5893.3703002

Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology, 30*(1), 55–72. https://doi.org/10.1007/s13347-016-0216-4

Tyler, T. R., & Fagan, J. (2008). Legitimacy and cooperation: Why do people help the police fight crime in their communities? *Ohio State Journal of Criminal Law, 6*, 231–275.

Wellford, C., & Cronin, J. (1999). *An analysis of variables affecting the clearance of homicides: A multistate study*. Justice Research and Statistics Association.