Guide to SecureDrop

Charles Berret

Columbia Journalism School

Tow Center for Digital Journalism
A Tow/Knight Guide

Funded by the Tow Foundation and the
James S. and John L. Knight Foundation

Acknowledgments

The Freedom of the Press Foundation provided tremendous support for this project, so my first words of gratitude are for its staff. My introduction to SecureDrop came when James Dolan spent a whole afternoon guiding me and a colleague through the process of installing the system on virtual machines. At a time when dozens of news organizations were waiting in line for similar attention, this was a remarkably generous gesture. Later, as my research project was just getting off the ground, Garrett Robinson's patient and often quite eloquent explanations of the SecureDrop system helped me to understand the level of care brought to developing it. Likewise, Conor Shaeffer has a gift for clarifying operational security measures while maintaining the full force of their complexity. I am incredibly grateful to Trevor Timm, who not only offered hours of interviews and commented on a draft of this report, but also brokered introductions to many journalists.

Interviews with these journalists formed the core of my study. I would like to thank Mike Tigas and Scott Klein of ProPublica, Barton Gelman of the Century Foundation, Julie Tate and Steven Rich of The Washington Post, Kevin Poulsen of Wired, John Cook of Gawker, Lydia Dennett of the Project on Government Oversight, Jeremy Keehn of The New Yorker, Micah Lee and Betsy Reed of The Intercept, and Alasdair McKie of The Globe and Mail.

My interviews with the technical administrators of SecureDrop systems also provided essential context to this study. I would like to thank Dave Boxall of The Guardian, Pam Rutter of the Project on Government Oversight, and Dan Phiffer of The New Yorker.

My doctoral colleagues at Columbia all helped me to develop and refine the ideas in this report: in particular, I would like to thank Jonah Bossewitch, Andi Dixon, Max Foxman, Alex Goncalves, Joscelyn Jurich, Travis Mushett, and Ri Pierce-Grove. Among my teachers, Michael Schudson, Todd Gitlin, Matthew Jones, Mark Hansen, and Dennis Tenen have had a particularly strong influence on how I see the concerns at play around this topic.

Above all, I am indebted to the Tow Center for Digital Journalism, which funded, guided, and published this research. Emily Bell listened to my pitch one evening over a year ago, warmly encouraging me to submit a proposal—

but also offered a "five-minute threat model" citing the substantial hazards of such a project. Fergus Pitt helped me shape the frame of my research as I was just getting started, then Claire Wardle offered indispensable guidance on my methodology as I performed the bulk of the work that follows. Susan McGregor was not only a mentor and a fellow traveler, but really paved the way for studying digital security and journalism. Pete Brown, Kathy Zhang, Smitha Khorana, and Nushin Rashidian have been a joy to work with at Tow. Finally, and perhaps most importantly, Abigail Ronck was a thorough and thoughtful editor. This report reflects the generous contributions of everyone listed above, but any remaining errors are my own.

May 2016

Contents

Secure Communications

Definitions, Terminology, Technical Introduction

The fields of cryptography and cybersecurity are awash with arcane and highly technical language. In the following section, I will attempt to demystify some essential concepts and place them in the context of tools like SecureDrop.

Cryptography is the process of rendering a message unreadable to all but the intended audience. In its original, readable form, a message is called *plaintext*. The means of encryption, or rendering it unreadable, is called a *cipher*. A cipher takes plaintext and combines it with a piece of secret information, called a key, to produce the encrypted message, or *ciphertext*. The proper key is required to decrypt the ciphertext back into the original plaintext. A *cryptosystem* is the ensemble of tools and processes needed to send and receive encrypted messages.

Cryptanalysis is code breaking. Whether by statistical analysis or exhaustive guessing, cryptanalysis is any means of turning ciphertext into plaintext without possession of the key. When an adversary intercepts a message, they may try to break the code through cryptanalysis to learn its contents.

The grounding axiom of cryptographic theory is *Kerckhoff's Principle*, named after a nineteenth-century Dutch cryptologist. It states: A cryptosystem should remain secure even if everything about that system besides the key is public knowledge. The information theorist Claude Shannon later rephrased this principle more succinctly, stating that one should assume "the enemy knows the system."[1] This means that even if an adversary captures one of your encryption machines, or if your algorithm is open-source software, the adversary should not be able to decrypt your messages unless they have also intercepted your key. In short, the security of a cryptosystem should be based on the secrecy of the key alone.

Key exchange is the process by which the parties of encrypted communications share the keys to encrypt and decrypt the messages they will later send. This is traditionally the trickiest element of secure communication, especially in large organizations like the military. The strength of the cryptosystem is immaterial, of course, if the key is stolen while it is being

exchanged between parties. Since a secure channel seems to be needed for the transmission of the key itself, the ideal means of secure key exchange once seemed like an infinite regress problem.

The modern era of cryptography began with a novel approach to the problem of key exchange devised by Whitfield Diffie and Martin Hellman.[2] Previous encryption systems had all been *symmetric*, meaning that the same key was used to both encrypt and decrypt messages. Diffie and Hellman's solution was for each party to have a private key that is kept totally secret, and for both parties to use their private keys in a sort of handshake to establish a secure channel. Models like this are called *asymmetric* or *public key* cryptosystems.

A year after the arrival of Diffie-Hellman, a team of MIT researchers developed the RSA algorithm, an alternative, proprietary, public-key cryptosystem that became widely used for both encrypting and authenticating messages. With RSA, each user has a widely available public key and a completely secret private key. The public key is used any time someone wants to encrypt a message to a specific person, while that person's private key is the only thing that can decrypt messages intended for them. A freely distributed implementation of RSA called PGP was developed in the early 1990s and directly resulted in relaxed legal restrictions surrounding the use of encryption by average citizens. Much of the cryptography in SecureDrop and other secure communication systems relies at some level on PGP or related, free software encryption tools like GPG.

The MIT key server is a directory for posting PGP keys, and its records are used in this study as a proxy for the rate of adoption of encryption tools in different newsrooms. When someone creates PGP/GPG keys, they send the public key to one of these servers so that it can be found and used when someone wants to send them an encrypted message. All the major public key directories share data so that each key can be found and confirmed in multiple places.

Yet cryptography is just one element of cybersecurity. Systems can be compromised by many other means besides breaking codes or stealing keys. A computer's security measures can be circumvented if it receives malicious code, grants access to an unauthorized user, or elevates user privileges so that someone can execute commands beyond their intended limits. There

is a vast and thriving market for novel ways of exploiting software, called *zero day* vulnerabilities because they are not yet public knowledge. Once a vulnerability has been revealed, and presumably also patched shortly thereafter, the vulnerability is dated upward. The logic behind this system is that even a ten-day vulnerability will still affect a targeted system if it has not received security updates in a month.

Experts assess the risks and vulnerabilities of a particular system through processes called *threat modeling*, *security auditing*, and *penetration testing*. A threat model assesses the nature and likelihood of risks. A penetration test is an attempt to identify vulnerabilities by subjecting the system to realistic attacks. And a security audit is a comprehensive, professional assessment of the risks, weaknesses, and needed improvements for a particular system, often combining both penetration tests and threat models.

Hackers are typically classified as *white hat*, *gray hat*, or *black hat* according to their ethical stance. The popular, broadly alarmist sense of the word "hacker" generally refers to the black hats, who are motivated to exploit technological systems for amusement, personal gain, or sheer malice. White hats use many of the same tools and techniques as black hats, but they do so for the sake of identifying and correcting vulnerabilities. Gray hats either believe that black- and white-hat tactics are appropriate in different contexts, or they simply reject this strict moral binary.

SecureDrop is *free and open-source software*, meaning that every line of its source code is freely available to read, modify, and share. In order to emphasize that the "free" in this term refers not to cost but to freedom, some advocates prefer the term *libre* software. Along with SecureDrop, all of the leading secure communication tools like PGP/GPG and Tor are maintained as free/libre/open-source projects. From a security perspective, following Kerckhoff and Shannon, open code is considered a basic condition for trusting any cryptosystem. When the code is closed to the public, there is no way to know if it is well implemented, let alone if it contains a secret backdoor. Open code, on the other hand, can be assessed for vulnerabilities and improved upon by anyone participating in the project.

Executive Summary

This report offers a guide to the use and significance of SecureDrop, an in-house system for news organizations to securely communicate with anonymous sources and receive documents over the Internet. SecureDrop itself is a very young technology. It was developed over the last four years, beginning during the period when the WikiLeaks submission system was down and it was unclear how else whistleblowers could safely transmit large caches of data to journalists.

The history of SecureDrop's conception and development is thus entwined with some of the most striking moments in the recent history of digital journalism: the arrival of Julian Assange as a charismatic force calling for radical transparency; the remarkable life of the technology activist Aaron Swartz; the bravery of Edward Snowden in revealing the level of surveillance now exercised by government agencies worldwide; and the resulting alliance between journalists, activists, and hackers who wish to ensure the accountability of powerful organizations by publishing information in the public interest.

Through interviews with the technologists who conceived and developed SecureDrop, as well as the journalists presently using it, this report offers a sketch of the concerns that drive the need for such a system, as well as the practices that emerge when a news organization integrates this tool into its news gathering routines.

In general, I found a fairly narrow and consistent set of practices among the journalists using SecureDrop. Many organizations designate just a handful of employees to check their system, and these employees act as operators, in a sense, who monitor the inbox and distribute promising submissions to the reporter who is best suited to assess and potentially act on that information. This is by far the most common model for the coordination of SecureDrop in newsrooms, and it appears to be so common largely because these practices were imprinted at the time of the system's initial, guided installation by the SecureDrop developers.

Given its complexity, SecureDrop may appear at first like a radical new tool, but many reporters told me that it closely resembles many of the other channels newsrooms have traditionally made available for sources to contact them. The crucial difference is that SecureDrop restores the effectiveness of a reporter's privilege to protect their sources through prin-

cipled non-cooperation—such as refusing to testify in court—whereas pervasive digital surveillance has made this gesture effectively moot over the last decade. The reality is that when a reporter's source can be identified through digital traces, the prosecution does not even need that reporter to testify. One of the explicit purposes behind developing SecureDrop has been to restore the possibility for journalists to protect sources whose communication devices might otherwise expose their identities.

Still, most readers must be wondering whether SecureDrop has proved worthwhile. This is a difficult question to assess because journalists are wary of revealing information that could put a source in danger. Still, most of my informants, representing nine of the ten organizations studied here, confirmed that the system has been generally valuable as a reporting tool, if not particularly consistent. Many were not willing to disclose the specific stories that originated with tips or documents from SecureDrop, nor the frequency of these stories. Nearly everyone did confirm, however, that the technical and often tedious process of checking the SecureDrop inbox is worthwhile overall, both as a reporting tool and as a signal that their organization takes seriously the protection of its sources.

Introduction

SecureDrop is a platform designed to facilitate secure and anonymous communication between sources and journalists. It is a complicated ensemble of computers, running carefully configured software that can only be accessed through a specific and deliberate set of procedures. This is especially true on the journalist's side, where most of the difficulty is stacked by design. One must log into a specific computer just to check the inbox, then one must use a separate, totally isolated computer to view and print any documents that have arrived. The process for the source is comparatively simple, relying only on the user-friendly Tor anonymous browser, though this process still requires a specialized tool and the initiative to use it. Such a lopsided investment is quite deliberate: The primary value for the designers of SecureDrop is to minimize the risk that the source—by far more vulnerable than the reporter in the majority of cases—could be identified or their messages intercepted en route.

For whistleblowers, choosing to reveal sensitive material has always involved some level of personal risk, whether it means harassment, imprisonment, or even physical violence. But technology today is uniquely susceptible to monitoring that could endanger a whistleblower. We now know that using computers, mobile phones, and other digital communication devices is particularly hazardous for matters intended to remain private. Whether information is skimmed in transit or seized from a data center, any number of digital traces may identify and endanger whistleblowers. And when this information is gathered without a warrant, it is immaterial whether the leaked materials hold public value that justifies publication. SecureDrop provides a secure and anonymous channel for sources to speak to journalists from a position of relative safety.

At the time of writing, the Freedom of the Press Foundation (FPF) directory lists thirteen news organizations, three independent journalists, and eight nonprofit activist groups that are operating verified installations of SecureDrop.[3] The FPF estimates that there are currently thirty running instances, including some that are not yet public. The organizations studied in this report include *Gawker*, *The Globe and Mail*, *The Guardian*, *The New Yorker*, ProPublica, and *The Washington Post*.

This list in no way indicates the limit of interest in SecureDrop: More than eighty organizations are on the FPF's waiting list. These organiza-

tions are holding out for a guided installation not only because it is technically demanding to set up the equipment, but also because many journalists will need assistance developing practical routines to make effective use of the system. In short, the purpose of a guided installation is both to limit the possibility of errors and security compromises, and to develop sound routines for checking and making productive use of the system. This leads to a fairly narrow set of practices surrounding SecureDrop. Unlike most other new and emerging technologies, which are subject to varying degrees of play and experimentation in their early stages, SecureDrop by its very nature is often used within a fairly limited scheme of preconceived practices.

The purpose of this report is to sketch the use of SecureDrop at this nascent but promising moment in its development, and to assess the role it serves alongside other means of encrypted communication available to reporters and their sources. To this end, I have conducted interviews with twelve journalists and three technical administrators at ten organizations using SecureDrop, as well as five people who are actively building the system and training journalists to use it. Although small, this group reflects a fairly comprehensive survey of SecureDrop's present user base as of early 2016.

It is worth noting that the interviews for this report were often complicated by the sensitive nature of the project itself. I began this work knowing that the use of SecureDrop in newsrooms would be a difficult phenomenon to examine. This is precisely why it seemed worthwhile to investigate. Still, my conversations were circumscribed by rigid borders. Not only were reporters wary of saying too much, but I was also bound by ethics (and the guidelines of my Institutional Review Board) to recognize that I could be placing others at risk, perhaps without even realizing it. The landscape of security hazards is broad and often largely unknowable, even for a system as carefully designed and thoroughly tested as SecureDrop.

The level of secrecy surrounding the system is, of course, deliberate. SecureDrop is designed to conceal as much as possible about the ways journalists and sources use it. At the time of this writing, the developers have commissioned five separate professional security audits to find and correct vulnerabilities. Unlike many other encrypted communication systems,

which are not just difficult to use but often used incorrectly, SecureDrop minimizes the possibility for journalists and sources alike to misuse the system and reveal identifying information.

The SecureDrop login and submission pages are only accessible via the Tor web browser, which conceals both the users and the sites on its network. If you were to fire up a Tor browser and click through to a SecureDrop submission page, you would see a page inviting you to log in, send messages, and upload documents—all with massive forces of encryption protecting your identity, location, and the contents of your transmission. On the other side, journalists log into their own special-purpose computers to check the inbox of messages and documents that sources have deposited through SecureDrop.

Despite the apparent intensity of these security measures, many journalists using SecureDrop say that the system is more than just a lure for high-impact stories: It reflects a commitment to do their utmost to protect sources who place themselves in danger for the greater public interest. Whatever the actual level of risk for the source or the sensitivity of what they have to share, a news organization offering SecureDrop is signaling its respect for the level of protection that their source demands. Given what we know (and don't know) about systems of mass surveillance today, this is a category of concern to which journalists have become increasingly attuned.

As a result, many journalists were understandably cagey about discussing SecureDrop. Every single person I contacted for this study must have at least considered the possibility that my stated intention as a researcher was a falsity—that I could be working for "the other side." And even if my intentions were genuine, could these journalists trust me not to commit a serious error in my handling of information? Could they even trust our channels of communication? Of course not. The essential foundation of a digital security mindset is a judicious and highly informed sense of paranoia. And our interviews threatened to introduce a needless security hazard to a system that is otherwise painstakingly hardened against attacks.

In short, it was clear that my informants treated the possibility of revealing sensitive information about sources quite seriously. This meant

that most of them would not identify the stories that originated with information from SecureDrop. Although the majority did confirm that it had happened and continues to happen, few would discuss the details of reporting these stories. Information on their patterns of use, not to mention the details of individual communications, could be enough for an adversary to try to identify the source of a particular story. In the wake of the Snowden revelations, these threats are not only plausible but fairly likely. Consequently, some interviewees preferred to speak in generalities about their process of assessing and then potentially acting upon tips that arrive through SecureDrop.

So how does SecureDrop affect a newsroom once it arrives? Are there new roles, reporting practices, or institutional configurations where SecureDrop is used?

Many of my informants explained that, as a point person using SecureDrop, they only monitor the system. If anything promising appears, they direct it to the reporter covering the relevant beat. Consequently, these point people often know very little about how the reporting process plays out from there—that is, how the beat reporter verifies documents, follows up on tips, and develops a broader picture of the issue at hand before filing a story. Whatever the novelty of SecureDrop, these aspects of the traditional reporting process remain largely intact.

Occasionally, a single, technologically sophisticated reporter assumes responsibility for the whole SecureDrop system. These rare cases require little coordination and have a minimal effect upon the greater newsroom. If the reporter leaves, the SecureDrop simply goes offline.

But in most of the newsrooms where I spoke to journalists using SecureDrop, the process seems to be integrated at some level into the greater newsroom. It is treated as a highly technical and sophisticated but largely quotidian technology. It sits alongside many other devices that journalists use to monitor information that may lead to further reporting. Like any other information source, it is neither a guarantee of valuable leads, nor a channel worth ignoring. SecureDrop appears to serve a unique and often narrow, but decidedly useful role in the newsrooms using it.

A Word on GlobaLeaks

Readers who have followed the development of secure whistleblowing platforms may wonder why the GlobaLeaks system does not receive consideration in this report. SecureDrop and GlobaLeaks share many qualities in common—both were designed to facilitate secure communication with whistleblowers; both are based around the Tor anonymous web browser; both have been audited by security firms to test for weaknesses; and both are free and open-source software developed to serve a role resembling that of WikiLeaks. From a technical standpoint, GlobaLeaks is also considerably less trouble to install than SecureDrop, which could be advantageous in many circumstances. But the reality is that GlobaLeaks is not being used by news organizations in the United States, Canada, or Great Britain, which together form the empirical scope of this research. On the other hand, GlobaLeaks has established a foothold in the Netherlands, where fifteen news organizations collectively support a fork of the GlobaLeaks system called PubLeaks. Given that SecureDrop is the only secure whistleblowing system being employed by news organizations in the English-speaking world, however, it is the only platform addressed in this report.

A Brief History of the SecureDrop Project

At the 2014 Hackers on Planet Earth (HOPE) conference in New York City, a panel announced the SecureDrop system as "a WikiLeaks for every newsroom."[4] It was a provocative and topical proposal at an event held in the wake of the Snowden disclosures, but many people must have been asking: Why would every newsroom need its own WikiLeaks?

By the time the SecureDrop project was first conceived in 2012, WikiLeaks itself was dealing with a staff mutiny, a shuttered submission system, and Julian Assange's self-imposed exile. Disaffected former staff had launched a new project, OpenLeaks, but it failed to gain comparable traction. In short, there was not a clear successor, even as news audiences still had an appetite for the brand of radical transparency that WikiLeaks had pioneered. For Edward Snowden to orchestrate his leak of NSA documents, it was necessary for him to devise his own digital security scheme from publicly available tools. Using Tor, PGP encryption, an anonymous email service called LavaBit, and a well-timed getaway, Snowden engineered the safe delivery of the files to a handpicked selection of journalists during the early months of 2013, right when the first prototype of SecureDrop was launched as another solution to the momentary decline of WikiLeaks.

The SecureDrop project was originally devised by Kevin Poulsen, a senior editor at *Wired* magazine and onetime fugitive hacker himself. Poulsen had noticed that journalists were facing a gap in the news ecosystem that Assange had so rapidly cultivated. "It bothered me that we had no dedicated channel for people to communicate with us securely," Poulsen said. "WikiLeaks at one point had a useable system, and it seemed like if they could do it, there should be a way for journalists to do it as well." But Poulsen envisioned an arrangement distinctly different from Assange's "middle-man" approach: He wanted to place this secure whistleblowing platform in the newsroom itself.

So Poulsen reached out to Aaron Swartz to collaborate on this project. Swartz was well known as an information activist and gifted computer programmer. He had been an author of the RSS protocol at age fourteen, a founder of the website Reddit, an architect of the Creative Commons licenses, and one of the most ardent and vocal activists opposing the Stop Online Piracy Act (SOPA).

Writing in *The New Yorker*, Poulsen described Swartz as "a member of a fairly small tribe with the skills to turn ideas into code—another word for action—and the sensibility to understand instantly what I was looking for: a slightly safer way for journalists and their anonymous sources to communicate."[5]

At the time, Swartz and Poulsen called their project "DeadDrop," in reference to a common element of spycraft. A dead drop is a designated, hidden site where documents or messages can be dropped off and picked up without participants ever needing to meet in person or know each other's identity. Similarly, the DeadDrop system was conceived to be an encrypted, anonymous space where whistleblowers could safely deposit sensitive documents for journalists to retrieve and assess for publication, without the whistleblower's identity being exposed. Swartz and Poulsen collaborated on the project in their spare time over the course of 2012, meeting to work in person only once at the *Wired* offices in San Francisco.

Unfortunately, DeadDrop would be one of Swartz's last projects. The first version of the system was finished in December of 2012, just a month before Swartz's suicide in a Williamsburg, Brooklyn, apartment at age twenty-six. Throughout the process of developing SecureDrop, Swartz had been under federal investigation for attempting to download the entire archive of academic articles from the subscription service JSTOR. His death is often imputed to the overzealous prosecution of intellectual property laws that Swartz himself had battled to prove unjust.

After Swartz's death, Poulsen helped move the project from *Wired* to another Condé Nast publication, *The New Yorker*, where it launched under the name "Strongbox" in May of 2013. That day, staff writer Amy Davidson characterized the system as a much-needed asset. "Readers and sources have long sent documents to the magazine and its reporters, from letters of complaint to classified papers. But, over the years, it's also become easier to trace the senders, even when they don't want to be found," Davidson wrote. "Strongbox addresses that; as it's set up, even we won't be able to figure out where files sent to us come from. If anyone asks us, we won't be able to tell them."[6]

But with Swartz gone, the project's code base was effectively abandoned. Without continued development, it was unclear if the system would ever

become straightforward and robust enough to use beyond the prototype developed within Condé Nast—even though Poulsen had intended from the beginning for the code to be released open-source and used in other newsrooms.

After several months of uncertainty, the project found new caretakers when the Freedom of the Press Foundation asked Poulsen if it could adopt DeadDrop and continue its development. Just one year earlier, the FPF had been founded by two members of the Electronic Frontier Foundation (EFF), the lawyer Trevor Timm and the technologist Micah Lee. The duo launched the FPF largely as a crowdfunding site for journalism organizations focused on transparency—especially WikiLeaks, whose donation services had been blocked by many leading payment companies. Lee would eventually help Laura Poitras and Glenn Greenwald learn to use encryption so they could communicate with an especially cautious source, Edward Snowden. In short, the FPF had already situated itself at the nexus of those concerns that grounded Poulsen's project, so he trusted the foundation to carry it forward.

First, Timm and Lee renamed DeadDrop as SecureDrop, and redesigned the interface from its original appearance—a white-on-black, cloak-and-dagger aesthetic—into something lighter and friendlier looking. The objective, after all, was to make the software more broadly usable and appealing. The FPF also made several hires in order to support the development of SecureDrop. These included the security expert James Dolan, who had helped design the original DeadDrop project with Swartz and Poulsen at Condé Nast, and a new lead developer for SecureDrop, Garrett Robinson, who had previously worked at EFF and as a security engineer at Mozilla.

After adopting the project, the FPF also commissioned a professional security audit to find any vulnerabilities that they would need to address as they pushed the software forward. They hired some of the best: security expert Bruce Schneier and a team from the University of Washington. That team spent thirty hours just trying to install SecureDrop before giving up. Although the group saw no obvious security flaws, this trial clearly highlighted that the system was far too difficult and idiosyncratic in its present state to be useful to others, let alone in the average newsroom.

In all, the FPF team spent about ten months disentangling, hardening, streamlining, and automating the SecureDrop code before releasing the first working version (besides the original, still running at *The New Yorker*). In October of 2013, the first SecureDrop systems were installed at Forbes and BalkanLeaks. ProPublica followed in January 2014. By the summer, when SecureDrop was billed at HOPE as a "WikiLeaks for every newsroom," there were over a dozen instances of SecureDrop running at some of the world's leading newspapers and activist groups. At the time of writing, about thirty SecureDrop systems are running at news organizations and activist groups worldwide, with over eighty on the FPF's waiting list for a guided installation.

Why SecureDrop Matters

With SecureDrop systems installed in a handful of prominent newsrooms, it is worth taking a critical look at whether—and if so, why—such a tool is needed. After all, the system is difficult, time consuming, and highly technical. Many news organizations may not have a staff member capable of using it, nor the resources to hire someone.

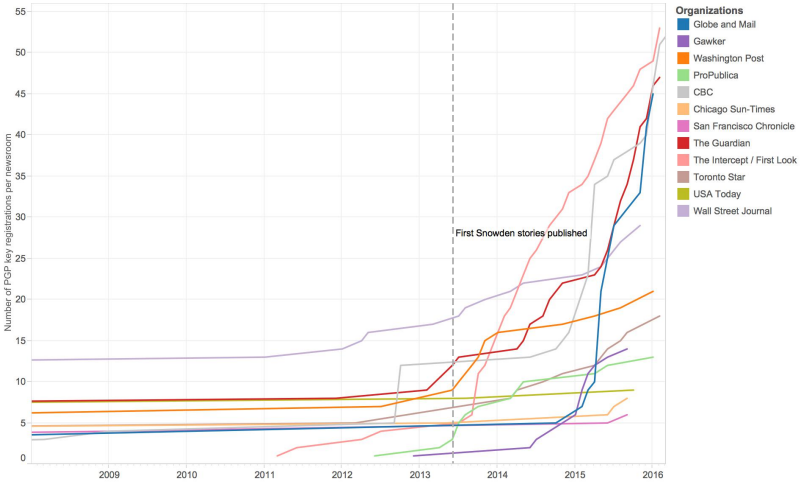
This section will outline the principle security concerns for journalists, the answers that SecureDrop provides, and the general framework in which those capacities will be interpreted in later chapters.

Digital Security Practices in Newsrooms

After Edward Snowden's disclosure that the majority of web traffic is gathered and surveilled by government agencies like the NSA, concerns about computer security were no longer limited to the discourse of hackers and privacy activists. In particular, journalistic interest in this subject gained new urgency as the duty to protect one's sources appeared to be increasingly difficult to fulfill. A Pew poll from February 2015 found that sixty-four percent of investigative journalists believe that they have been subjected to surveillance by the U.S. government.[7] The same poll found that about half of these journalists had since taken measures to protect sensitive documents they share, and thirty-eight percent had begun to use secure communication tools with their sources.

Data from the directory of encryption keys at the MIT key server also supports the increasing use of encryption tools among journalists.[8] For this study, I searched for keys registered to email addresses at a selection of news organizations, including those running SecureDrop.[i] The figure below shows the running total of PGP key registrations at some of the few news organizations represented in the key directory. This figure also includes an index line noting the date of the first published Snowden disclosures. Although this event is probably not the sole cause of the rising use of encryption among these journalists, it is clear that there has been a drastic change from the relative flatline in most newsrooms beforehand.

i. Please see the appendix for more on data and methodology.

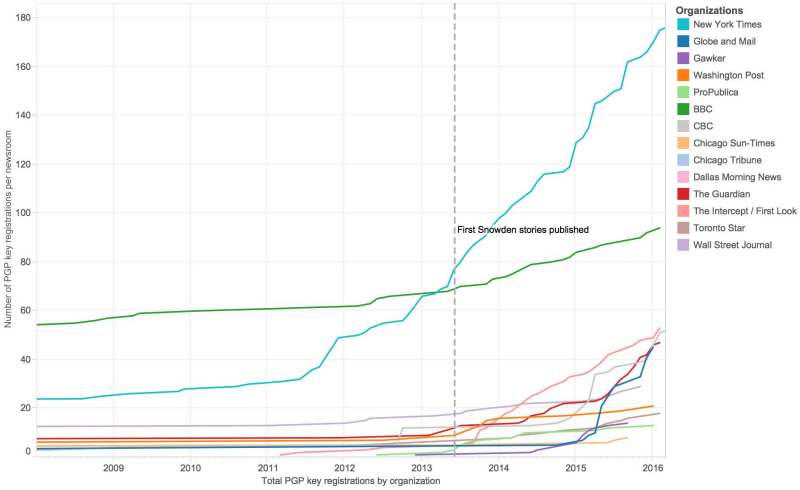


A selection of news organizations and the number of their employees who have registered encryption keys at the MIT public key server over time.

It is worth noting that journalists' adoption of encryption tools has been highly uneven: The vast majority of news organizations have no listings at all in the directory. The major outliers are *The New York Times* and the BBC, neither of which has a SecureDrop system in place. Nevertheless, both have had a large number of employees register PGP keys at the MIT directory over the last seventeen years—though their lines are omitted from the graph above because they throw off the scale. While the BBC rate of encryption-key registration has been fairly consistent over the last fifteen years, *The Times*'s numbers began to climb at a faster rate in 2011; it surpassed the BBC in early 2013, right before the Snowden disclosures.

The bar graph below shows the total number of PGP key registrations at each of the news organizations I pulled from the MIT key server. The table lists the number of registrations each year over the past decade.

Although these numbers provide some sense of which news organizations have recognized the uses of encryption versus those which have ignored it, these totals should not be read as raw indicators of digital security consciousness from place to place. The BBC's total of ninety-four PGP key registrations reflects just half of one percent of its 18,974 total staff. On the



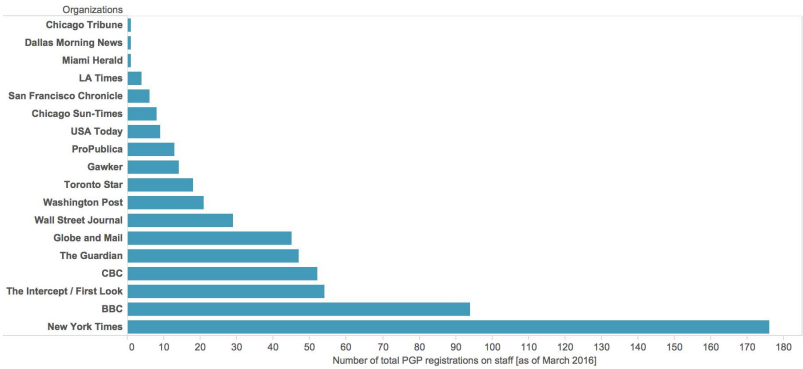
The graph above with *The New York Times* and BBC included.

other hand, ProPublica's thirteen registrations represent nearly a quarter of its sixty employees.

Bearing in mind this limitation of the data, it is worth noting that the benefits of increased PGP registration across newsrooms are not necessarily cumulative. In the past, news organizations with just one or two journalists set up with encryption have been contacted by sources who specifically wanted to work with them. What is more problematic is the large number of news organizations in which encrypted communication channels are completely absent, or where interested reporters do not have the opportunity to be trained.

Anecdotally, several of my informants observed that the overall use of digital security tools in their newsrooms appeared to increase after the installation of their SecureDrop system. When the FPF developers visited to oversee the installation of the SecureDrop system, then returned to check up on it, these conversations sometimes prompted further steps among the staff to encrypt hard drives, set up PGP keys for encrypting email, and download the Tor anonymous browser or the Tails anonymous operating system.

Still, this elevated attention to security rarely extends beyond the small group of reporters who are trained to use the SecureDrop in each news-



Total public key registrations by organization.

room. "That wasn't something that we thought would scale to the whole newsroom," said Alasdair McKie of *The Globe and Mail*. "We really needed to identify, who are the most invested recipients of that training, who are most likely to take it to heart and actually use it in their day-to-day lives as reporters."

Comparing Encryption Systems

While the growing use of PGP encryption among journalists is a strong signal that digital security has become a greater concern in the wake of the Snowden disclosures, the contents of those disclosures suggest the limitations of encrypted email for protecting sources.

Like many secure and encrypted communication tools available today, encrypted email tends to protect only the content of messages. "There is a pretty big ecosystem now of secure communication tools, but there are very few that deal with anonymity and metadata protection," said Micah Lee of *The Intercept*. "And the reason is that this is a much, much harder problem. A much easier problem, relatively speaking, is encryption."

The array of metadata that accompanies an encrypted transmission over email, phone, or chat is not only enough to prove that the communication has taken place, but also to pinpoint the parties, time, duration, frequency, location, and the presence of files transmitted in the message. In

	Date										
Organizations	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
BBC	1		2	3	2	1	1	5	7	9	2
CBC				1	1			8		4	7
Chicago Sun-Times									1		
Gawker								1		2	8
Globe and Mail										3	4
LA Times										1	
Miami Herald							1				
New York Times				2	3	2	19	10	36	24	16
ProPublica								1	6	3	
San Francisco Chronicle					1						
The Guardian							1		5	9	
The Intercept / First Look							2	2	8	21	2
Toronto Star								1		6	
USA Today									1		
Wall Street Journal							1	3	4	2	1
Washington Post		1						1	8	2	

Number of employees at each organization who registered public keys each year from 2005 to 2015.

some cases, this has been enough information not only to identify a whistleblower, but to prosecute.

"Not every source is an expert on being an anonymous source," Poulsen said. "That's not why they're contacting a reporter. It's because they're an expert on something else."

Timm framed the problem another way: "You can't teach sources to be secure, because you don't know who the sources are."

SecureDrop is designed to be as easy as possible for sources to use, while still requiring them to take reasonable security precautions. Because SecureDrop runs as a Tor hidden service, potential sources can only access its submission system while they are under the anonymity protections of Tor and, ideally, also the Tails secure operating system.

SecureDrop is particularly useful for facilitating a secure, anonymous first point of contact between the source and journalist—which is a largely unsolved problem in terms of secure communication. As Timm explained it: "You have to make that first contact, and that first contact is almost certainly going to be insecure, so SecureDrop is a way to have that point of first contact." Oftentimes, after beginning a conversation on SecureDrop, the journalist and source may choose to move the conversation to another, more convenient venue like encrypted email, chat, or phone calls.

For the journalist, this is especially valuable because it is better to know your source's identity, even if you do not plan to reveal it.

Still, the basic nature of digital security is that threats can never be totally eliminated, only minimized along a greater number of possible avenues of attack. This has remained the case over the long history of cryptography, but it is compounded by the complexity of digital communications systems today. Even the strongest encryption scheme can be circumvented through the idiosyncrasies of software design and network pathways, not to mention that users can easily and unwittingly make mistakes while using these tools.

Garrett Robinson, the lead developer of SecureDrop, said:

> With a lot of this stuff, we don't have a clear sense of what an adversary could do, and so a lot of our thinking is just to make things harder for them. It's hard for us to say, "This solves a problem." It's more like, "This raises a bar for an adversary." But it's not reasonable to assume that they can't get around it.

Poulsen noted that these dangers can be further minimized because SecureDrop is a single-purpose system. "If you're receiving tips on the same system that you are using to send and receive routine emails, that's poor architecture. That's not a good idea," he said. "So that was the idea originally behind SecureDrop. Here, we're going to have one little box that does nothing except stay secure, stay updated with patches, and be utterly dedicated to this one purpose of handling sensitive communications. And that is something that nobody had before."

Legal Protections of SecureDrop

"People think of SecureDrop as a technical tool," said Timm of the FPF, "but it's almost as much a legal tool." He pointed to the recent history of journalism to explain the specific needs that SecureDrop was designed to address. Since the 1970s, he said, journalists had banded together and produced "one of the most effective civil disobedience campaigns since the Civil Rights era." They effectively refused to testify against sources and would voluntarily go to jail to avoid doing so. This led many states to pass shield laws, which protect the reporter's privilege not to disclose their interaction with sources. There is not yet a federal shield law, but many

federal circuit courts at least provide some limited privilege for journalists based on the First Amendment.

In leak cases during the Obama administration—the largest number filed under any U.S. president—none has required a reporter to testify. In the James Risen case, one reporter was subpoenaed, but federal prosecutors eventually dropped the subpoena and then easily convicted the source using electronic records from the government.

"I think a major reason that there have been so many prosecutions of sources in the past decade," Timm said, "is that the government figured out that they didn't need reporters to testify against their sources anymore."

The legal advantage of SecureDrop is that the servers reside on the media organization's property. Thus, no one else has access to it. When both the source and the journalist are using this system to communicate, they are only connecting to the server on the newsroom premises. There are no third parties who could be subpoenaed to release information, so the news organization can conceivably return to fighting battles over reporter's privilege even if information is communicated over a digital channel. Timm explained:

> Let's say *The Washington Post* publishes a blockbuster story and they say that SecureDrop was used—or the government thinks SecureDrop was used. If they want to subpoena someone, they need to serve it on the news organization, and that means we can re-trigger the right that these organizations have lost over the past decade, which is that they will have the ability to challenge the subpoena before handing over the information—to go to a judge and say that this violates the First Amendment. They will have the ability to appeal it and ultimately reserve the right to be held in contempt of court rather than hand it over.
>
> This will really make the bar for the government a lot higher. Number one, maybe the government just won't issue the subpoena in the first place, because they know it will be difficult and they won't want the public fight. Number two, even if the news organization ultimately loses after a years-long court battle, hopefully SecureDrop collected so little data on the source that it would be useless to the government anyways.

By comparison, even the strong protections of encryption systems like PGP email only conceal the contents of messages. They do not conceal the fact that communication has taken place between two parties, and in some

cases that may be enough to endanger the source. No matter how difficult it is to break the encryption, if your source sends an email from anything besides a personal server, there is little to stop either eavesdropping on the transmission of that message or the seizure of records from the provider. SecureDrop solves both of these problems.

A Rare Exception to Post-Industrial Journalism

The fact that SecureDrop must reside on the premises of each news organization makes it somewhat unique among the new tools and platforms that journalism organizations use to connect with the public. Many journalists and their employers now post their stories to social media sites like Twitter or Facebook, which currently serve as some of the most influential portals for readers to find news and entertainment.

For Emily Bell, professor of Journalism and director of the Tow Center at Columbia, this indicates that news organizations are losing control over their distribution channels as more of their work is consumed through a network of social media platforms. "Social media and platform companies took over what publishers couldn't have built even if they wanted to," Bell wrote in a recent piece for the Columbia Journalism Review. The choices the companies running these social networks make—on matters like whether to permit ad-blocking software—may now be the main factor in determining the fates of publishers.[9]

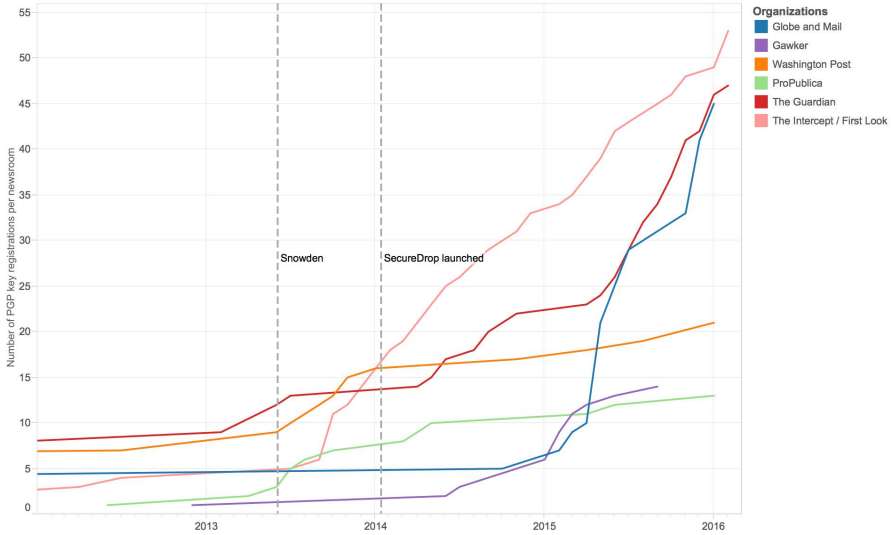
SecureDrop is a notable exception to this state of affairs—sometimes characterized as a move toward "post-industrial journalism"—in which news organizations allow outside parties to manage more of the gathering and distribution of their content.[10] The SecureDrop servers must reside within the newsroom, first and foremost because this location is under its control and is granted the legal protections the US affords to its press. If the organization placed the system on a server farm, or used any seemingly secure communication platform run by a third party, its data could be seized without any consideration for the effect it might have on the freedom of the press. This seizure could also happen without their knowledge.

SecureDrop, by working to restore the press protections that have proved

elusive in the context of digital media, is at once an undeniably advanced technology, and also one developed to reassert the past conditions of journalistic practice. The SecureDrop system cannot be outsourced without losing the key pillars of its security model, so its place in the newsroom is fixed even as the conditions of post-industrial journalism may rapidly push other fixtures of the newsroom further afield.

Case Studies: News Organizations Using SecureDrop

In order to understand the landscape of different newsrooms using SecureDrop, the following section outlines case studies of five organizations: *The Intercept*, *The Washington Post*, *Gawker*, *The Globe and Mail*, and ProPublica. PGP registration numbers for these five organizations plus *The Guardian* can be compared in the graph below.



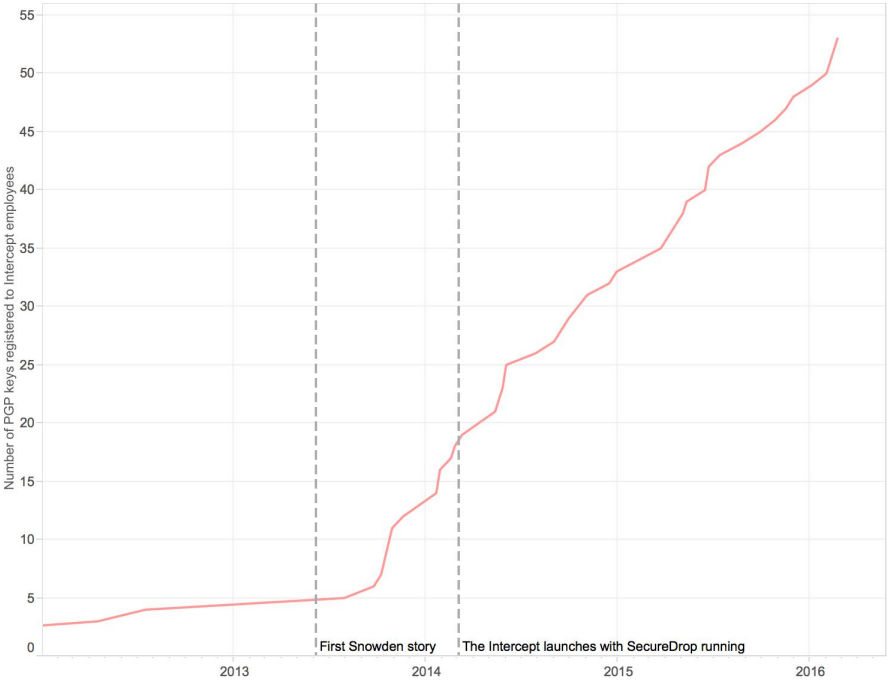
Public key enrollments over time at a selection of organizations using SecureDrop. Please note that due to differences in total staff at these organizations, direct comparisons are difficult.

The Intercept

The Intercept is an online publication established in the wake of the Snowden disclosures by eBay founder Pierre Omidyar. Many of its current staff reporters and technologists were involved in reporting these disclosures, including Glenn Greenwald, Laura Poitras, and Micah Lee. Consequently, *The Intercept* is unique among news organizations in its focus on digital security, including mandatory training for its staff.

The organization's concern for security is borne out by the large number of staff members enrolled on the MIT key server. The graph below shows

the accumulated total registrations among employees of *The Intercept* and its parent company, First Look Media.



Number of public key registrations over time at *The Intercept* and First Look Media.

Beyond its large footprint on the MIT key directory, *The Intercept* is also notable because it launched in early 2014 with SecureDrop running from day one. Lee, one of the founders of the FPF and one of the developers of SecureDrop, not only set up *The Intercept*'s system, but was also the sole staff member checking it for some time.

Recently, a "centralized group" has joined Lee in reviewing submissions and distributing materials when a source is trying to contact a specific journalist. Betsy Reed, the editor of *The Intercept*, described this as a time-consuming but manageable process. "We had to get into a rhythm for checking the SecureDrop. It works best to do that on a rotating basis because there can be a high volume of material to get through, but we've gotten into that rhythm."

Reed also confirmed that her organization has had an increasing level of success with SecureDrop. "Especially recently, as awareness grows of its existence, we've seen more and more good stories coming out of that pipeline," she said, adding, "but as with any kind of tip line at any news organization, the vast majority of leads we get, they don't pan out."

Lee echoed that while *The Intercept* frequently receives tips and documents in its SecureDrop system and that a fair share of them warrant further reporting, they pass on the majority of material. "It's very frequent that we get contacted through SecureDrop and the information we have is kind of interesting, and we talk about it for a while, but then we decide that it's not interesting enough to warrant doing more journalism around it, or publishing anything," he said. "Because, you know, most sources don't have incredibly juicy stories for you. That's pretty rare."

Like other publications studied here, *The Intercept* does not make a practice of acknowledging when the source for a story contacted the outlet through SecureDrop. The first exception came in November 2015, when *The Intercept* published a story about a company called Securus that provides phone services to prisons. The journalism hook was that Securus was recording phone calls between inmates and their lawyers in violation of attorney-client privilege. The lede paragraph stated:

> The materials—leaked via SecureDrop by an anonymous hacker who believes that Securus is violating the constitutional rights of inmates—comprise over 70 million records of phone calls, placed by prisoners to at least 37 states, in addition to links to downloadable recordings of the calls.[11]

Lee explained that the decision to reveal the use of SecureDrop in reporting the Securus story was the result of assessing the potential risk to the source, who dropped out of contact shortly after delivering the documents. "In this specific case, we looked into it and we couldn't see any harm that could be done to our source, or our source's identity, by saying that it came from SecureDrop. We don't know the actual identity of our source, but we were able to validate the information." Two weeks later, *The Intercept* posted a second story with direct acknowledgement that it was based upon documents sent through SecureDrop, but these acknowledgments are still rare.[12]

Reed underscored that these decisions are not specific to SecureDrop: "We have to evaluate the risks of disclosing any details about sourcing—including whether it comes via Securedrop—on a case by case basis, taking into account when possible the source's assessment of their own risks, but also making our own independent assessment."

The Washington Post

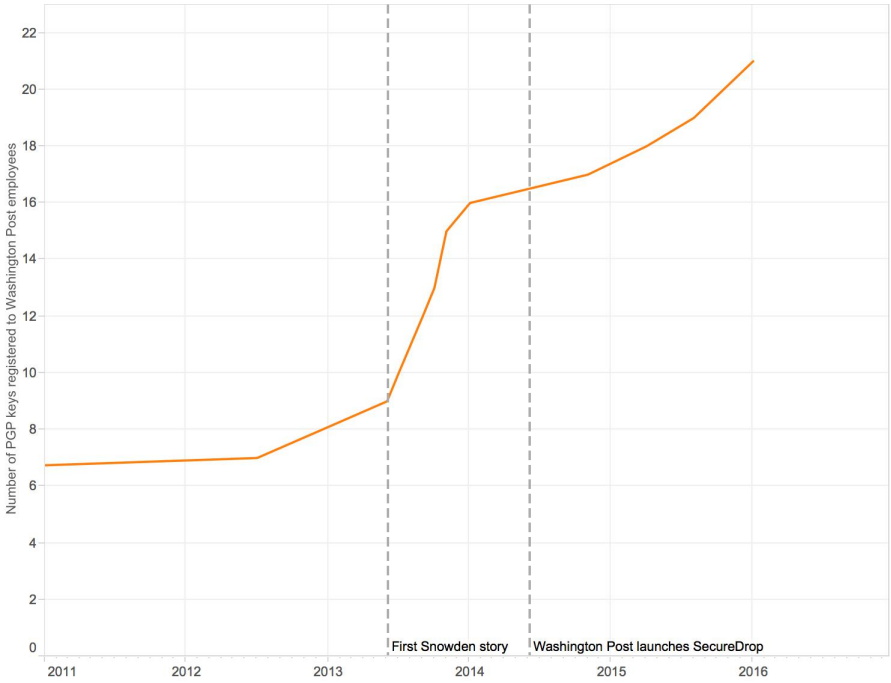
For Barton Gellman, one of the reporters who handled the Snowden disclosures for *The Washington Post*, learning to use encryption tools only proved useful after much waiting. "I published my first PGP key in 2006," Gellman said. "I was up and running with encryption and Tor for seven years before Edward Snowden found his way to my inbox. He could not have reached me if I had not left out the welcome mat." Gellman now runs his own personal SecureDrop at the Century Foundation, but *The Post* itself was also an early adopter of SecureDrop, launching the system in June of 2014.

The Post appears to have developed an efficient system to monitor its SecureDrop. According to Steven Rich, a database editor for investigations at *The Post*, they have a team of three journalists who gather, assess, and distribute tips to reporters around the newsroom. Trevor Timm of the FPF even surmised that *The Post* may have the "best coordinated" system among all the organizations currently using SecureDrop.

When asked if SecureDrop has been successful at *The Post*, Tate replied, "Definitely. I can't go into what those stories are. But we've had success with it, definitely."

"We spend a fair amount of time trying to figure out what something is and where it should go," said Julie Tate, one of the journalists who monitors the SecureDrop at *The Post*. After delivering each tip, Tate and the other point people will respond to the source through the SecureDrop interface to let them know a reporter is looking into it. They also give some expectation of how further contact will be coordinated if the story moves forward.

"If I hook up a reporter with a source, often I'm not involved anymore—one hundred percent of the time I'm not involved anymore," Tate said. "I'm like, this is what we've received, this is how this person can commu-



Number of public key registrations over time at *The Washington Post*.

nicate with you—you know what I mean? It's like introducing two people, and then I step out. I'm just facilitating people communicating with each other."

Rich said that interesting tips tend to receive about a week or two for pre-reporting before a full investigation is launched. "You don't generally get entire stories leaked," Rich said. "You get the tip of the iceberg."

Rich also noted that most people in *The Washington Post* newsroom are aware of SecureDrop, but the majority don't use it. Moreover, he said that many reporters mistakenly think they do not need it. "Most people work with more sensitive things than they think they do," Rich explained.

Although the majority of the newsroom may not use SecureDrop, others are using tools like PGP instead. According to Tate, all of *The Post*'s foreign reporters use encryption tools of some kind. Data from the MIT key server reveals that the enrollment of Post reporters with encryption keys

increased noticeably after the Snowden disclosures were published, while the installation of its SecureDrop system appears to have had little effect.

Gawker Media

Gawker Media, a company operating a network of single-subject blogs, promotes its SecureDrop system with considerable bravado. Each day, an automated post lists the various channels through which a source might choose to contact them:

> Don't forget: You can email us tips at tips@Gawker.com, call them in at 646-470-4295, send them directly to any of our writers, or use our anonymous SecureDrop system.

John Cook, executive editor of *Gawker* Media, said that adding SecureDrop to this post was a natural extension of their usual efforts to gather material from readers:

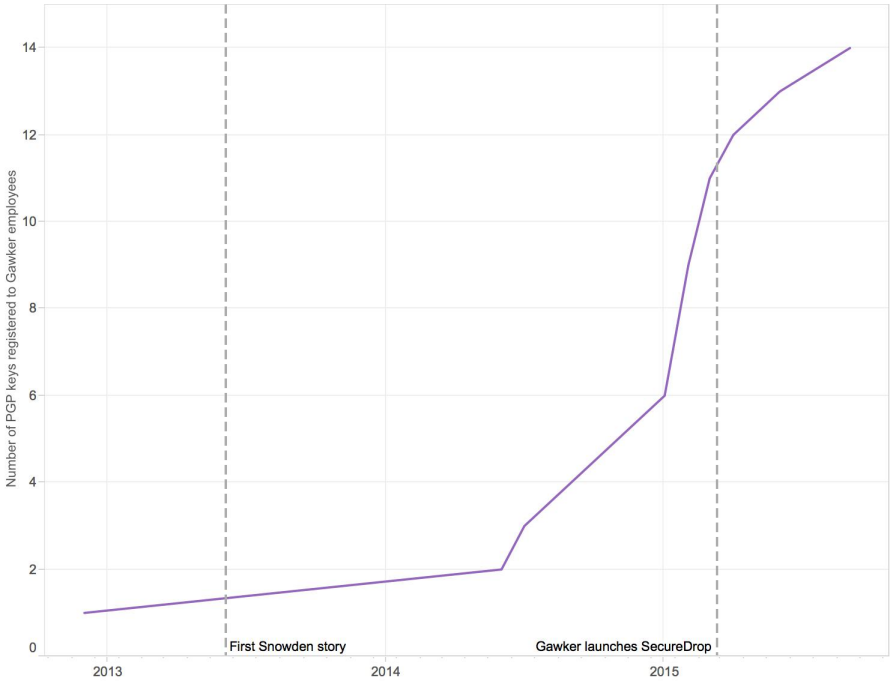
> That was always there just to get tips through email or our phone tips line. So this was a daily post that went up—we call them blips—that go up in the daily flow of the site just to remind people how to contact us, how to send us tips, and so when we got SecureDrop set up and installed we added SecureDrop to that blip across all the sites just to remind people that it's there.

Cook admitted that *Gawker*'s SecureDrop is particularly prone to unwanted and often grotesque submissions. "Aside from people sending us cat videos and stuff, we do have an army of very dedicated trolls coming after us." Cook added that this class of submission is "probably pretty unique to *Gawker*, or at least more energetic when directed at *Gawker*."

According to Cook, who worked at *The Intercept* before returning to *Gawker* Media, his staff has an established routine to check SecureDrop for promising tips. "We have three people who are trained on checking it," he said. "They check it and then write up an email report every day about what's in it, and send it around to a limited group. And then we just go from there on what to pick up on, and who to respond to, and who to communicate with."

Cook added: "We just treat these as tips and farm them out to people who are available and suited to pursue the story."

Columbia Journalism School



Number of public key registrations over time at Gawker.

When asked about the character of the useful tips in its SecureDrop, Cook said that they receive a "healthy variety of material," but that the bulk of journalistic material tends to be directed at "*Gawker*" itself, its sports blog "Deadspin," its feminism blog "Jezebel," or its automotive blog "Jalopnik."

Asked whether the platform has proved useful as a reporting tool, Cook said yes, and elaborated that his staff has been working on a long-running and potentially promising investigation based on a tip from SecureDrop: "The best one—which I wouldn't feel comfortable talking about—is something that we're still working on, and it's been a long-term thing, but I don't want to talk about it."

Like many publications, the number of *Gawker* reporters registering public encryption keys jumped in recent years, noticeably in the months preceding its installation of SecureDrop. Although a total of fourteen *Gawker*

employees are on the MIT key server, Cook said that only about five of them use encryption regularly.

The Globe and Mail

In March of 2015, Toronto's Globe and Mail installed the first SecureDrop in Canada. In an article announcing the launch, *The Globe*'s editor-in-chief David Walmsley wrote, "SecureDrop is the 21st-century equivalent of the manila envelope: It provides you with an anonymous venue for relaying material you believe to be in the public interest and you have no other way to get it out publicly."[13]

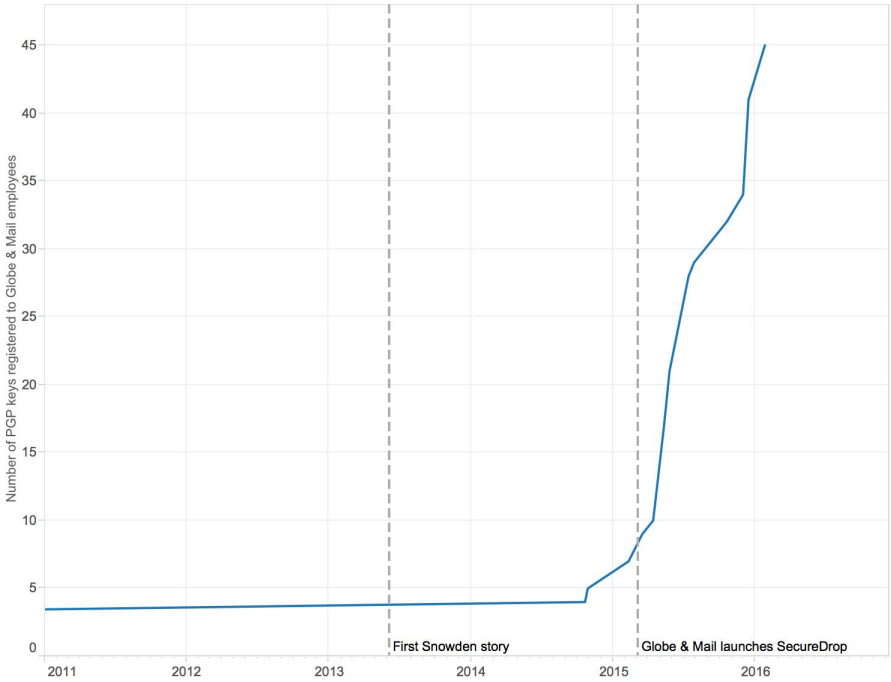
Deputy production editor Alasdair McKie, who is one of the primary caretakers and facilitators of *The Globe*'s SecureDrop, said that the system quickly proved itself useful, yielding a story almost immediately after its launch. The use of the system is largely tied to *The Globe*'s investigative team. A handful of these reporters have been trained to use SecureDrop and check it roughly three times a week for promising material.

McKie's account of messages received in its SecureDrop also suggests that *The Globe* might be less afflicted by spam and trolls than other news organizations. "The majority of the submissions that we've received, I would call good faith submissions from potential sources," McKie said. He continued:

> They're not intentionally wasting our time. They're not intentionally sending us something that's not of journalistic value. They're not sending us garbage on purpose just to yank our chain. That is not super common. It does happen. But it's not something that's been a problem for us.

Like most other informants in this study, McKie declined to point to specific cases in which tips and documents from SecureDrop led to published stories. Furthermore, he said that *The Globe* established an explicit policy before launching SecureDrop that their organization would never, under any circumstances, indicate that a source had come through this particular channel.

Beyond its use as a reporting tool, McKie also highlighted that running SecureDrop reflects an awareness of our society's present surveillance dilemma and a respect for the press's role in highlighting this reality:



Number of public key registrations over time at *The Globe and Mail*.

> The fact that there are people who are willing to contact us over SecureDrop, who are not willing to contact us through another avenue, underscores for people not just the editorial leadership in the newsroom, but also just the company in general, that information security is a fact of life now. And some of the other initiatives, like getting people signed up with PGP keys and that sort of thing, is something that is going to be part of our lives. And the sooner we incorporate that into the way we go about our business, the better it is for news organizations, in particular, because we are the focus of policy-making information in our society.

According to records at the MIT key server, only a few Globe and Mail staff members were registered with PGP before their organization's SecureDrop was installed. McKie said that many of the advances in security training in their newsroom took place in preparation for the installation of SecureDrop. Records also indicate that the majority of Globe PGP keys were registered in the months following the launch of its SecureDrop. Dur-

ing the 2015 calendar year, twenty-eight more of the paper's journalists registered PGP keys, placing *The Globe* in the top third of organizations studied here in terms of total registrations. It ranks just ahead of *The Wall Street Journal* and just below the *The Guardian*.

ProPublica

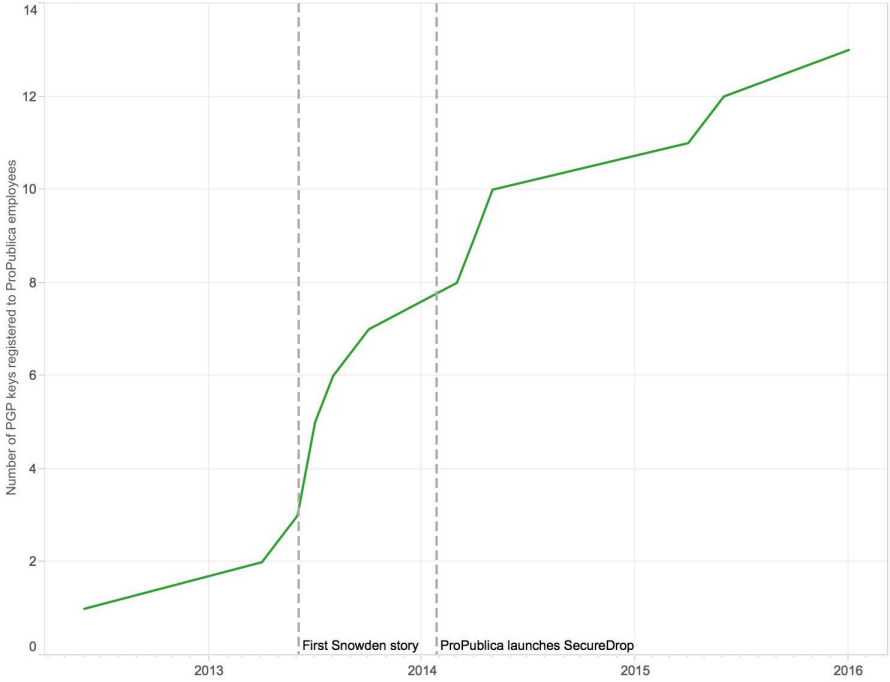
ProPublica was the third organization to install a SecureDrop system after the FPF rebooted the project, and yet it was also the only organization whose representatives stated that SecureDrop has not been a particularly successful source of stories.

Instead, ProPublica staff articulated a broader spectrum of uses for SecureDrop. Assistant Managing Editor Scott Klein said: "We don't see SecureDrop exclusively as a way for anonymous whistleblowers to send us the proverbial plain brown envelope' full of data, because that's actually a pretty rare event. We also see SecureDrop as an ideal way for sources we know to send us data and documents in an environment where the anonymity and security are turned up to eleven."

For instance, a source was communicating with a ProPublica reporter over encrypted email to exchange a cache of documents but found they could not transmit such a large volume of data due to the brute limitations of the email system itself. ProPublica's reporter then advised the source to deposit the files through SecureDrop instead. In this case, SecureDrop was neither a first point of contact nor, in a strict sense, an anonymous one.

Mike Tigas, who maintains ProPublica's SecureDrop, said he logs in to check the system about once a week, and that the whole process takes about an hour. Tigas said that a few useful tips have come through messages dropped into the system, but none of these have become an active, repeat source. He estimated that a new source comes to ProPublica's SecureDrop with a potential story about once a week, but that these are rarely useful leads.

Asked whether ProPublica would cite SecureDrop in the event that a major story originated in the system, Tigas said there isn't a firm policy in place: "We haven't had too many of these situations and we publish slowly enough that I think that decision will continue to be made on a per-project



Number of public key registrations over time at ProPublica.

basis. We'd definitely consider touting SecureDrop if the circumstances were right."

Tigas also noted that many ProPublica reporters prefer to use PGP email for sensitive conversations because they are working with known—rather than anonymous—sources. He estimated that about ten reporters regularly use PGP with a total of about fifty regular sources. Based on the key server registration figures, ProPublica's enrollment had a slight spike after the Snowden revelations and once more after the outlet installed SecureDrop.

Typology of Submissions and Newsroom Practices

Based on the accounts outlined in earlier chapters, several themes emerged that characterize the general experience of using SecureDrop. For one, materials that gravitate to SecureDrop inboxes tend to fall into a handful of distinct categories. The routines, practices, and general perception of SecureDrop also tend to be fairly consistent across organizations.

Categories of Submission: What Turns Up in SecureDrop?

"The ratio of wheat to chaff is unsurprising," said Barton Gellman. His personal SecureDrop received more than five hundred messages in the twenty months between July 2014 and January 2016. Of those, he said about one hundred unique user names were registered, but these did not necessarily indicate unique visitors. Overall, Gellman said that fewer than ten percent of his SecureDrop contacts provided "useful information," but of these only three contacts were able to provide him with "significant and journalistically valuable" information. It bears repeating that three whistleblowers in less than two years is still a considerable success rate. Nevertheless, for the sake of source protection, journalists are often not at liberty to describe the worthwhile materials they receive—whether these are troves of spreadsheets, images, PDFs, or emails they review for veracity and journalistic value.

Consequently, the journalists I interviewed were far more willing to discuss the junk they receive. The following section outlines categories of common submissions that need to be discarded in search of useful journalistic material in SecureDrop.

Security Testing

Several informants said that some of the most common messages to populate their SecureDrop inboxes arrive from white-hat hackers performing security tests on the system. Gellman said that many messages explicitly state that they are merely "checking the system setup for flaws or confirming it is online." The SecureDrop developers do offer a "bug bounty" for those who find flaws in the system, so these messages are most likely sent in

order to check for potential information leaks or openings where the system may be breached.

Malware

Despite the intense precautions of the SecureDrop developers, some submissions arrive harboring malware. Gellman noted that it is especially important for journalists to be wary of file types where malware is commonly hidden, such as PDFs and DOC files. Gellman specifically recounted catching malware in several submissions to his SecureDrop. "One upload consisted of what purported to be a long list of stolen credit card numbers, and there was malware embedded in the submission," he wrote in an email, adding that "there have been three other confirmed deliveries of malware. Those could have posed a meaningful risk to the security of the system, but I do not (ahem) run executable files."

Spam

As with any system where submissions are unfiltered and unmonitored, there is essentially no way to eliminate spam from SecureDrop. Cook of *Gawker* recalled being subjected to an especially nasty barrage of unwanted messages when his system first got off the ground. "When we launched, we were beset by trolls, so there were a lot of horrible images of dead bodies, and porn, and people uploading massive videos just to gum up the system and take up time," he said. "The first three or four days checking it were just a nightmare." Although these sources of noise are perhaps unavoidable, many outlets said the level of spam they receive is low and easily managed.

Tips of Limited Value

Mike Tigas said that ProPublica's SecureDrop does not receive "spam" in the sense of "people trying to mess with them," but that irrelevant submissions result more often from people trying to act as sources when in actuality they don't really have anything of journalistic value to share. This seems to be due to an ordinary lack of news judgment.

McKie of *The Globe and Mail* shared a similar account, but also defended the value of tips that may not be offering secret or previously un-

known material, because these may alert reporters to what readers consider important. "Sometimes just the fact that they sent it to us is enough to kind of twig us, journalistically, to a potential story," he said.

Tate of *The Washington Post* echoed this:

> Sometimes it is very confusing, because people are sending you pages from a published book. But what they're trying to do is put context around those pages. You know, it's not like they're sending you a page from a book and saying that this should be a secret communication. They're saying, "Look at this page in this book and let me explain to you what is happening here."

Conspiracy Theories

Other failures of news judgment receive little sympathy. Many journalists are all too familiar with messages from an eager source with no credible evidence to back up their claims. SecureDrop seems to be particularly inviting for these sources. Gellman said that he has received about twenty unique communications from people offering him "elaborate and implausible theories."

The majority of my interviewees confirmed receiving this category of submission, but Tigas of ProPublica said he encounters messages like these no more than once a month. Cook of *Gawker* seemed more accepting and even somewhat entertained by these characters: "SecureDrop is very wonky and labor intensive. It's difficult and it's a pain in the ass. By nature, it attracts people who are paranoid and distrustful. So interacting with the people who come to you through that channel, it's always interesting."

McKie of *The Globe and Mail* noted that SecureDrop may actually have a slightly higher signal-to-noise ratio than other channels the public may use to contact journalists:

> We've had the newsroom telephone line for decades and it's always been called the "crank line," and there's a reason for that. SecureDrop doesn't change that. If anything, SecureDrop raises the barrier to entry so that people have to work a little bit harder to get in touch with us, but if you compare SecureDrop to other means, people seem to be a lot more motivated. They're not just doing it for fun, and as a result what you get is people who believe, for whatever reason, that there's a story in what they've sent you.

Hoaxes and Fakes

A separate genus of unreliable stories includes those that are deliberately false. Gellman said that he was contacted by a "sophisticated fabricator" offering forged documents using a "well-planned and well-executed fake persona," which took Gellman some time to debunk. This underlines the importance of approaching material in SecureDrop, like anything else, with proper skepticism and subjecting it to rigorous verification. In Gellman's case, this was time consuming, but he also said it was "a net positive for me as a learning exercise."

Over the Transom

One of the interesting properties of SecureDrop is that it essentially offers a direct connection to an editor. Many writers covet this level of access, especially when they are accustomed to submitting their work to slush piles heaping with other literary hopefuls. At *The New Yorker*, for instance, editor Jeremy Keehn said that when they first launched SecureDrop, "more than half of the submissions were fiction or poetry." None of these submissions were accepted for publication in *The New Yorker*, and Keehn encouraged these writers to use conventional channels in the future.

Newsroom Practices

According to my interviews, the uses of SecureDrop fall into a fairly narrow set of practices. This is due, in part, to the design of the system. It is engineered to limit the possibility of security failures, which necessarily means limiting the range of possible actions for users. This much is logical and unsurprising. But the on-site installation and training from the FPF appears to be an equally important factor in the range of practices by SecureDrop users.

Checking the System and Distributing Tips

In most newsrooms, a group of four or fewer reporters is tasked with checking the SecureDrop at least once a week. The most common rate of checking reported was three times weekly. Once they have identified promising

submissions, the reporter determines which of the organization's reporters is best suited to assess and follow up on the tips or documents received.

The exception to this check-and-distribute model is with personal SecureDrops. Poulsen views his SecureDrop as a tool he offers for people who specifically want to contact him. He said that he checks his system "regularly" and that it gets "plenty of use," but he declined to offer details of his interactions with sources. Gellman also gives a fairly generous level of attention to those who leave messages on his personal SecureDrop. "I generally respond to every submission that is not essentially empty or pure trolling," he said. "I find that people are grateful and sometimes surprised to hear back."

There is also no guarantee that a journalist will hear back from a source after their first appearance in the system. For this reason, some organizations said that they would attempt to move the conversation off SecureDrop and onto another, more convenient encrypted channel as soon as possible after the first point of contact. Otherwise, there is a risk that a useful source will disappear and not return to carry on the conversation, even if the reporter wants to push forward with the story.

Verification

Like any tip or document, materials in SecureDrop must be subjected to journalistic verification. Cook of *Gawker* said the process is exactly what one would expect in traditional scenarios. "There's nothing unique about the SecureDrop system," he said. "It's the same thing we do with anything you get, which is you do regular old reporting to verify it—to see if it will stand up."

Rich also pointed to a traditional journalistic skillset for assessing what arrives in *The Post*'s SecureDrop: "Throughout investigative reporting," he said, "you get a sense for what tips you can use and which ones you can just throw away."

One aspect of verification that journalists may not have at their disposal when using SecureDrop, though, is the identity of the source. Poulsen said:

> My preference as an old-school journalist is that I like to know who I'm talking to. But part of the idea behind SecureDrop is that in this age right now, it's harder to make guarantees that somebody's identity is going to re-

> main secret. The government has so many ways of surveilling journalists—and they show a willingness to use it—that I think the bar for accepting information from somebody whose identity is a mystery even to the reporter, I think that is now by necessity a bar that we reach more easily than in the past.

Nondisclosure of SecureDrop Stories

Although most journalists using SecureDrop told me they consider it a useful reporting tool, they were mostly unable to disclose the stories that originated with information from sources on SecureDrop. Thus, it could easily appear as though the journalistic footprint of SecureDrop is rather small.

McKie of *The Globe and Mail* said that they take a strict editorial stance on this point: "Before we launched SecureDrop, we adopted the explicit policy that we would not acknowledge that it was the source for any given story."

To date, *The Intercept* is the only publication to have acknowledged when published stories have arrived through SecureDrop.[14] They have since acknowledged a total of three in print, but Lee maintains that these are not the only Intercept stories to originate with tips or documents from its SecureDrop.

Cook of *Gawker* added:

> It's kind of a Catch-22 in that one of the things I've always wanted to do is to say, "Hey, we got this through SecureDrop." But you don't want to do that, because you don't want to do anything that would lead someone to try to go look if someone's work laptop has Tor on it, or whatever might lead to suspicion.

Placing SecureDrop Alongside Other Communication Channels

Another theme that has emerged from studying SecureDrop is that while it is at once progressive and technologically advanced, it also stands in the spirit and defense of longstanding, traditional reporting methods. Many journalists said that SecureDrop tips are just like any other tip and that the technology is very similar to others in its basic efficacy.

McKie of *The Globe and Mail* specifically characterized SecureDrop as a channel alongside other channels:

> When we were pitching this idea to our newsroom leadership, one of the things that we were careful to point out is that the purpose of SecureDrop for us is to provide a door into the newsroom, alongside all of the others. We're not telling people to stop calling us, we're not telling them to stop emailing us, we're not telling people to stop mailing us the generic manila envelope or sliding it under the door. All of the ways that people are getting in touch with us are still valid, it's just that in this day and age, there are certain kinds of sources who don't feel comfortable using those kinds of means anymore—and potentially, with really good reason.

Additionally, journalists often weigh SecureDrop against other channels when they are considering how to handle sensitive documents. Rich of *The Washington Post* said, "For large files, I would prefer a physical hand off, especially for something that sensitive." This highlights a point worth remembering: Even with a tool as advanced as SecureDrop, it is wise to consider the entire range of approaches at your disposal when security is a concern.

Conclusion

I spoke to representatives of ten news organizations for this study, and nine told me that they regularly receive useful tips or publish stories based on information provided to them directly through SecureDrop. Still, one of the questions that looms over SecureDrop, much like any unfamiliar technology, is whether it is worth the trouble.

One of the ironies inherent in SecureDrop, and perhaps in any technology that facilitates anonymous leaking, is that its openness both enables the collection of incredibly valuable information that could not have been attained otherwise, and also attracts absolute garbage that most reporters go to considerable lengths to keep as far from their desks as possible. The same anonymity measures that protect vulnerable sources from danger make it practically impossible to block, filter, or otherwise discourage those with nothing valuable to share.

Nevertheless, most reporters were adamant that the trouble of installing and maintaining a SecureDrop system has been worth it, whether it is measured on journalistic value, financial return, or moral principle.

McKie of *The Globe and Mail* said that when the question of installing SecureDrop was first raised in the newsroom, they crunched the numbers for the equipment and installation expenses, as well as for the regular labor hours that the system would require. "We decided that it was a relatively small amount of money," he said, "and if we got one story out of it, we would consider that a success—and anything else was gravy."

McKie added that the first SecureDrop story arrived "pretty much immediately," and that the system has proved consistently useful over its first year—although, like my other informants, he was not willing to disclose which stories or exactly how many *The Globe and Mail* has published based on material gathered through SecureDrop.

Cook of *Gawker* voiced a similar sentiment:

> It's a hassle, but it's worth it, even if it's just one story a year. And a big part of it, for me, was just messaging to our readers and our community that we take security seriously, and that we're investing our time and resources into ensuring that for the exceedingly small fraction of our readership that actually has information to share, and the inclination to do it, that there's a way for them to do it that safeguards their identity.

Gellman also underlined the importance of opening secure channels to

provide for sources who would not contact the press otherwise. In his case, the source was Edward Snowden, who reached out to Gellman because he was one of the few reporters using PGP email at the time.

And even though Snowden's case is pointed and quite persuasive, it is worth foregrounding other reporters' insistence that secure communication tools like SecureDrop would be worthwhile even if it did not yield blockbuster stories. "Nobody's expecting to get another Snowden just because we set up SecureDrop. There may never be another Snowden," said McKie. "We always have to be aware of the fact that not every source we get through SecureDrop is going to have some massive, earth-shaking revelation, but there are definitely more Snowdens out there in the sense of people who will not get in touch with us unless we give them this option, as opposed to the other options."

Framing SecureDrop this way highlights its need as both humble and urgent. Source protection is a basic and essentially undisputed journalistic value. But the legal and technological considerations to meet this need have become dramatically more complicated as unchecked powers of surveillance have been tacitly granted to several world powers. SecureDrop is not meant to amplify or augment the reporting capabilities of a newsroom, but rather to help ensure the conditions of source protection that are necessary for a healthy press.

"The way that I conceived it, this is not a dangle to lure people into giving you stories that you would not otherwise have gotten," Poulsen said. "It's a system that is set up just for you to communicate with me safely. So if people are using SecureDrop instead of sending me an email, if they're using it instead of calling me on the phone, then SecureDrop has proven its usefulness right there. And the answer to that is yes, they are."

Appendix: Data Gathering and Cleaning

Data on the number of PGP key registrations in each newsroom was gathered by scraping the MIT key server in March of 2016.[15] Registrations on the MIT server have considerable, if not total, overlap with other key servers because they synchronize data with one another.

Each employee was identified by the supplied email address attached to their news organization. Three concerns should be noted here: Anyone can register a PGP key to a particular email address, even if they do not own that account; new email addresses can be added to a registry at a later date; and not every journalist who is using encrypted email will be doing it on their work account. These are the main limitations in the coverage of the data presented here.

Other problems, such as duplicate entries, were fixed by manually cleaning the data. Many people, over time, have registered several different keys. Some people register more than one in a single day, perhaps in the midst of a tutorial. Many others choose to revoke an existing key and register a new one at some point in time. Whatever the case, duplicates were eliminated from this report's data, wherever possible. Each entry in which two or more keys were registered under the same name, or under clear variations of one person's name, were also manually deleted. Only the earliest registration was maintained so that timelines would not include later registrations from the same individual. Thus, each entry should reflect their earliest enrollment with encryption keys.

This condition has one notable but largely unavoidable effect on the data: Sometimes a security-savvy reporter will move to a new organization but their entry is still counted for their previous employer, where they first enrolled their encryption keys. It's worth emphasizing that the numbers associated with each organization should not be read as figures for total staff using encryption, but rather for the number of staff who enrolled their first encryption key at that organization. This number becomes less accurate and less useful at organizations with a longer history of registrations, such as those that stretch back to the 1990s.

Key registrations for a news organization are also not necessarily journalists. Especially in the earlier key registrations in this data set, it is clear that many were working in the information technology department. Thus,

some of these registrations do not indicate that an employee has set up encryption for the sake of communicating with sources.

Finally, entries for general addresses like contact@ or tips@ each site were removed. While these may be useful avenues for secure communication, they do not signal that a particular journalist has begun using encryption.

Citations

1. C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, no. 4 (October 1949): 656–715.

2. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, no. 6 (1976), https://www-ee.stanford.edu/~hellman/publications/24.pdf.

3. "The Official SecureDrop Directory," Freedom of the Press Foundation, https://securedrop.org/directory.

4. "HOPE X Schedule," HOPE, http://x.hope.net/schedule.html.

5. Kevin Poulsen, "Strongbox and Aaron Swartz," *The New Yorker*, 14 May 2013, http://www.newyorker.com/news/news-desk/strongbox-and-aaron-swartz.

6. Amy Davidson, "Introducing Strongbox," *The New Yorker*, 14 May 2013, http://www.newyorker.com/news/amy-davidson/introducing-strongbox.

7. Jesse Holcomb, Amy Mitchell, and Kristen Purcell, "Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior," Pew Research Center, 5 February 2015, http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/.

8. MIT, *MIT key server*, http://pgp.mit.edu/, http://pgp.mit.edu/.

9. Emily Bell, "Facebook Is Eating the World," *Columbia Journalism Review*, 7 March 2016, http://www.cjr.org/analysis/facebook_and_media.php.

10. Chris Anderson, Emily Bell, and Clay Shirkey, "Post-Industrial Journalism: Adapting to the Present," Tow Center for Digital Journalism, 3 December 2014, http://towcenter.org/research/post-industrial-journalism-adapting-to-the-present-2/.

11. Jordan Smith and Micah Lee, "Not So Securus: Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege," *The Intercept*, 11 November 2015, https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/.

12. Jenna McLaughlin, "U.S. Mass Surveillance Has No Record of Thwarting Large Terror Attacks, Regardless of Snowden Leaks," *The Intercept*, 17 November 2015, https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/.

13. Colin Freeze, "The Globe Adopts Encrypted Technology in Effort to Protect Whistle-Blowers," *The Globe and Mail*, 4 March 2015, http://www.theglobeandmail.com/news/investigations/the-globe-adopts-encrypted-technology-in-effort-to-protect-whistle-blowers/article23302598/.

14. Smith and Lee, "Not So Securus: Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege."

15. MIT, *MIT key server*.