San Francisco Open Email

Ben Cohen
bcohen@ischool.berkeley.edu

Master's Final Project
Advisor: Deirdre Mulligan
School of Information
University of California, Berkeley

May 6, 2010

Table of Contents

Abstract

The city of San Francisco is considering the email requirements of the various departments in the city, and looking at possible models for creating an "open email" system in which city email would be publicly searchable, in order to promote open government in compliance with the California Public Records Act and the Sunshine Ordinance. To better understand user needs and potential issues with this model, I conducted a series of interviews with members of the San Francisco Police Department. Through these interviews, I identified the current patterns of use of email within the department, and areas in which the department can improve its use of email.

Introduction

In December, 2009, the city of San Francisco issued a request for quote (RFQ) for "the analysis and compilation of business, technical and policy requirements, for the...email environment [of the city]," (Appendix 1). In addition to an assessment of the email requirements for the city, the proposal specifies that "the contractor will need to help define and evaluate the policy and technical implications of 'open email'," and further that there is to be a "case study of the Law Enforcement Agency email pilot project."

A multi-disciplinary team from the Center for Information Technology Research in the Interest of Society (CITRIS) at UC Berkeley, including faculty and graduate researchers from Boalt Law School and the School of Information, submitted a proposal in mid-December. The proposal describes two tracks of inquiry. The first is focused on "examin[ing] alternative approaches to achieving the City's goal to be 'an open and transparent organization' through 'open email'," through "technical, security, legal, and ethical analysis," (Quote and Proposal, CITRIS). The second track is an examination of the "Law Enforcement Pilot Program," specifically through qualitative research aimed at assessing the current uses and needs of the San Francisco Police Department (SFPD) with regard to email. Additionally, the qualitative research with the SFPD is designed to "analyze the social implications of various 'open email' systems and the consequences that user behavior may have for the overall openness and transparency of government, employee privacy, [and] efficiency," (Quote and Proposal, CITRIS). It is the second track that I was responsible for, and which is the focus of this paper.

Before discussing the research and its findings, it is important to understand what distinguishes email as a communication medium, and what "open email" means for San Francisco city government.

What is email?

The focus of my qualitative research with the SFPD was on the use of email as a communication medium. There are several features that, while not unique to email, are important to understand. For the purposes of this paper, the salient features of email, as a system, are that it:

- is asynchronous;
- allows one-to-one communication;
- allows one-to-many communication;
- requires a client that has the ability to communicate with the email server;
- can be used to communicate outside of an organization;
- does not allow significant recipient control over what is received;
- does not allow significant sender control over how a message is retransmitted;
- can be used to attach and share files;
- routes messages without realtime human involvement;
- results in messages being stored on the sender's machine, the recipient's machine, and at least one server in between.

These features distinguish it from other forms of electronic and non-electronic communication used in the SFPD. While not discussed in detail here, this list is a reference; each item on it has bearing for the themes and recommendations that arose from this research.

"Openness" in California government

Openness in government can and does mean many things. Typically, it involves granting the public access to government meetings and writings. At the federal level, the United States has the Freedom of Information Act (FOIA), passed in 1966, among other laws. However, many states have their own laws as well. In 2004, Californians voted in favor of proposition

59 (Prop 59, First Amendment Coalition), a proposed amendment to the state constitution which established public access to government information as a constitutional right (California Constitution, Article 1, Section 3).

The statutory right to government information has existed in California since well before 2004. In 1968, the California Legislature enacted the California Public Records Act (CPRA) (California State Government Code (GC), Section 6250-6270). The CPRA allows for anyone to request access to a public record. The CPRA defines a public record as "includ[ing] any writing containing information relating to the conduct of the public's business prepared, owned, used or retained by any state or local agency regardless of physical form or characteristics," (GC Sec 6252). The CPRA gives the public broad access to government information, but includes a number of voluntary exemptions, including exemptions for "[p] ersonnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy," (GC Sec 6254.c) and "[r]ecords of complaints to, or investigations conducted by, or records of intelligence information or security procedures of,...any state or local police agency," (GC Sec 254.f). As stated, these are voluntary, rather than mandatory, exemptions, and many, including 6254.f, are heavily qualified. Nevertheless, the CPRA seeks to strike a balance between the public's right to information and the competing interests such as the privacy rights of government employees and members of the public, such as the victims of certain crimes. Because of its history in the state, the breadth of its provisions, and the prevalence of claims made through it, I focused on the CPRA as the primary legal means for granting public access to government information in this research.

Current email landscape of San Francisco and the SFPD

As of May, 2010, the San Francisco's email infrastructure is highly heterogeneous. Each department within the city exercises significant control over how email is deployed, used, and managed. Although email addresses across the city belong to the same domain, sfgov.org, the email servers, clients, and policies are determined by each department. The SFPD currently uses Lotus Notes for its email system, and runs a separate Windows Active Directory server for user authentication for desktop login. Consequently, logging into email requires at least two usernames, and potentially two passwords, as well. About 1,600 members of the department have Lotus Notes email accounts, while about 1,000 members of the department have no officially issued email account. In parallel with my research, the SFPD participated in an email trial with Microsoft to test a hosted email system. The email trial was conducted in order to assess the suitability of the Microsoft hosted email solution for the SFPD. My research was designed to address the larger, encompassing, question of what needs of the SFPD need to be met by any future email system.

Research

Participants

In the spring of 2010, I conducted interviews with thirteen members of the SFPD. My liaison within the police department was Lieutenant Greg Yee of the Technology Division. In coordination with Lt. Yee, I was able to recruit participants from a wide range of ranks and roles within the SFPD, as well as a mix of civilian employees and sworn officers. Interviews took place at 850 Bryant St, which is the SFPD operational headquarters as well as the Southern Station, and the Taraval station, both in San Francisco. The participants include members of the Risk Management Office, the Investigations Bureau, the Golden Gate Division, the Technology Division, Staff Services, and the Police Commission. The

range of years with the SFPD ranged from a few years to over thirty. To preserve the anonymity of the participants their comments will be identified by participant number, as well as by the source of the comment, eg (P99, transcript) or (P99, notes).

Methodology

All of the interviews were conducted in person, either at the SFPD operational headquarters or the Taraval station. I used a grounded theory approach (Charmaz, 2006) to identify themes and guide participant selection along theoretical grounds. Ten of the thirteen interviews were conducted in a one-on one setting, and for the other three, I worked with another member of the CITRIS project team from UC Berkeley School of Law. The interviews were semi-structured, with some deviation to accommodate the wide range of roles and responsibilities of the participants. The interviews lasted between 45 and 120 minutes. Extensive notes were taken during each interview, and audio recordings were made for most of the interviews, except in cases where the participant did not wish to be recorded.

Limitations

There are several limitations to the research I conducted. While my close collaboration with Lt. Yee allowed for ready access to participants, I had little independent knowledge of the suitable candidates for each of the participant roles I wished to sample. Consequently, the participants I worked with were all deemed suitable, at least informally, by a representative of SFPD. Additionally, given resource constraints, interviews were conducted at two of the ten SFPD stations. It is possible that greater geographic diversity among the participants would affect the findings.

Findings

The findings from the interviews are divided into two sections. In the first section, I have identified themes in the current use of email by the SFPD. These include the reasons people use email, issues with the current system, and uses of technology outside what the department issues. In the second section, I've identified issues pertaining to privacy, transparency, and the use of email.

Current Use

Email use is socially contingent

The most reliable predictor of email use within the police department is the use of email by peers, either within or outside the department. Among participants with department issued email accounts, email is used to communicate with a wide variety of parties, including peers within a division, managers or superior officers, outside agencies, city attorneys, contractors and vendors, and the public. Participants whose interactions are primarily with other email users are most likely to prefer email as a communication medium. As one participant clearly put it, "I would say I prefer email for most communication," (P11, notes). The converse is also true. For participants with email accounts who interact primarily with members of the department who don't have email, it is not the preferred form of communication, regardless of whether a particular interaction could take place over email. One participant described this mindset particularly well:

> "In the world of police work, we're up-to-date as far as technology is concerned, but my personal belief... being a police officer is a different world. When you're on patrol, after the morning meeting, you hit the ground running." *(P7, notes)*

Because of the disparity of use within the department, participants situated at the boundaries between groups that use email extensively and groups that either don't have or

don't use email found email particularly problematic. These participants found they were often required to use email for reporting to their superiors (P7, P8, P13, notes), and were expected to respond in the same medium for those communications, but couldn't rely on email for communicating with peers or subordinates. Consequently, they tended to view email as an inconvenience that took time and attention, but offered little benefit.

Participants also valued sending and receiving email differently. Participants more often valued the ability to send email over receiving (P3, notes). In part this is due to norms of use and etiquette, as discussed below, but participants also attributed the difference to the asynchronous nature of email. The convenience of being able to send an email at any time became an inconvenience when it meant having to check email throughout the day.

Trust and reliability are critical factors when communicating

In police work, trust is critical. In many of the interviews, participants indicated that people are trusted, while machines are not. For important communication, interoffice memo (IOM) is the preferred means of delivery. This is especially true for sensitive or confidential information (P3, P6, P7, notes). Conversely, email is viewed as inherently insecure, "Anything can be hacked. It might just be a question of when," (P8, notes). One participant said she feels comfortable sending anything by email, but only because she knows and has independently verified the identities of everyone she corresponds with (P10, notes). Another way in which the difference in trust manifests is in participants' sense of chain of command. In explaining why IOM is preferred over email, a participant said, "With email, someone can send a message to anyone, and you won't know. With [IOM] you send it to your superior, and you know it follows the chain of command," (P3, notes).

There is nothing inherent to the technology that makes email less able to be sent in line with the chain of command, yet for many participants, there is something inherently untrustworthy about the medium. The same belief if was expressed by participants discussing sharing information with the public. Today, information that is shared with the public goes through a human filter in the police department. For some information, the filter is the legal division. For other information, such as police reports, the records clerk manages most disclosures. When asked about automated systems for sharing information with the public, participants were uncomfortable. As one participant said, "I'd worry if it were automated, something would go wrong," (P2, notes). Another had similar concerns, "My gut feeling is no, it isn't possible to have sufficient technical safeguards," (P11, notes).

In addition to the culture of the police department, which has long put trust in people and processes to ensure consistent, appropriate behavior, there is the question of accountability. Removing human actors from a system of information transmission and disclosure makes it unclear how to assign blame when there is a problem. At the recent Pervasive and Autonomous Information Technology (PAIT) conference in Cincinnati, this question was addressed directly. Since the mid-nineties, there has been work considering accountability in human-computer systems (Nissenbaum, 1994), but as technology gets more sophisticated, autonomous agents can perform many of the tasks previously performed by human actors. If the filtering of documents to be shared with the public is performed by a piece of software, who is accountable when something is shared inappropriately? Faced with this question, and no clear answer, the participants in these interviews expressed distrust of automated systems and preferred to rely on tested processes relying on human actors.

Related to the issue of trust is the issue of reliability. One reason cited by some participants for not using email is the time it takes. In many areas of the department,

computers are shared resources. For accountability, users must login to computers with their own, unique usernames. On some computers, this can take as long as ten minutes (P8, notes), since the department uses "roaming profiles" that must pull individual user data from a central server (P1, notes). After logging in to the desktop system, users must login to the email system, which requires a different username and password. If any of these systems is experiencing technical issues, the user is not able to send an email. Consequently, for users without dedicated computers, sending an email often takes ten times as long as making a phone call.

Lack of policy, training, and culture for email use

> "I don't know. We have a computer policy about what you can load on them, but I don't know that they've come out with thou shalt not email this or that." *(P8, notes)*

The provisioning and use of email within the department has been a slow and piecemeal process. One participant recalled getting an email account through the department as early as the mid-nineties, although it was not an sfgov.org account (P12, notes). Other participants still do not have email accounts. In the late nineties, the department adopted the Lotus Notes email system, which is still uses. The first, and only, general order (GO/DGO)[1]that discusses the use of email is 10.08, which was written in 2002. About that order, one participant said, "General Order 10.08 came out in 2002 and addressed the personal use of computers, what passwords should be on there, etc. That needs to be updated to address changes in technology and new equipment," (P4, notes). Most participants are not aware of the email provisions in DGO 10.08, although it is publicly availably. One typical response, when asked about whether there are any official policies regarding the use of email, is, "I'll have to plead the 5th on that. I'm not sure," (P8, notes).

[1] All General Orders can be found at http://sf-police.org/index.aspx?page=1720

Part of the issue is a lack of formal training on the appropriate use of email. Many participants expressed a positive view of the training offered by the department, but when asked about training specific to email, most could not recall training on the proper use of email. One participant recalled email "as another example of a medium in which we should not sexually harass coworkers. Something like that," (P11, notes). No participant could recall training about what information should be shared via email.

Despite the lack of official policy about appropriate use of email, many participants have developed a sense of what is appropriate to discuss over email, and how email ought to be used. However, many of these views conflict with the views expressed by other participants. Some participants send personnel files and other confidential or sensitive materials by email, while other participants said that it would always be inappropriate to send confidential material, including personnel or disciplinary matters, by email. Some participants like having the ability to send to many recipients, for example when sharing a weekly newsletter, while other participants feel that email should be sent to as few recipients as possible, as would be the case with interoffice memos. One participant captured this variety by saying, "San Francisco is unique. You'll find there's not one set way of doing things here," (P6, notes).

The lack of clear policies about the appropriate use of email is in marked contrast to the training and policy about how to write police reports. This may not be surprising, given how integral police reports are to the daily operation of the department, but there are important parallels between the two. Police reports are regularly released to the public through trials and public records act requests. Yet when asked whether they received explicit training about what information in police reports could be made public, most participants were not sure, with the exception of the names of domestic abuse victims, which all participants recognized as potentially non-disclosable. Instead, the SFPD has a 91 page report writing

manual instructing officers the correct way to write police reports, and a general order (GO 3.16) specifically about the release of police reports to the public. The department has taken great care and invested significant effort in training officers the correct way to write reports without burdening them with the legal intricacies of public release. Email is also subject to public records act requests and discovery in trials, yet there is no equivalent training offered.

In addition to email, police have a variety of alternative media for communication with electronic text. Besides department issued email, officers have the ability to send text messages through the Computer Assisted Dispatch (CAD) system in the patrol cars, the Web Workstation software provided on all desktops, an intranet based messaging system, and for some members of the department, PIN messaging on department issued Blackberry devices, SMS via personal cell phone, and email via non-department issued email accounts. There are varying levels of auditing, control, and access to all of these systems, and no participants were aware of training or policies addressing the appropriate use of these technologies for conducting police business.

Individuals have access to technology beyond what is provided by the department

The SFPD has employs many technologies in the service of more effective crime prevention. Nevertheless, there are many technologies available to the general public that are not fully deployed within the police department. In some cases, when a technology offers tangible benefits, individuals use technologies that aren't purchased or deployed by the police department, and use those technologies in the fulfillment of their duties with the police department.

In general, cell phones are not provided to officers by the police department. Between thirty and forty members of the department have officially issued Blackberry devices

(Meeting with city, notes), but these are typically issued lieutenants, captains, and members of the command staff or technical staff. Nevertheless, many patrol officers carry personal cell phones that they use in the course of duty (P9, notes). Patrol officers have several forms of communication available to them, including their mobile vehicle terminals (also know as mobile data terminals or mobile data computers, MVT/MDT/MDC) and radio. However, several participants said that many patrol officers use cell phones to communicate with other officers on patrol, with the station, and with members of the community.

Cell phones are especially well suited to communicating with the public, and in Ingleside, there has been an experiment to provide beat officers with cell phones paid for by local businesses (SF Examiner, 2009) (P13, notes). Cell phones are also useful when there is a code 33, indicating that the radio is tied up (P13, notes), or when an officer needs to contact a specific colleague, such as a officer responsible for dealing with issues in the homeless community. In addition to being used for communication, modern cell phones can provide services not otherwise available, "I prefer to communicate via cellphone... It has tools you can use, maps, navigation... It would help out a lot if the computers in the cars had GPS. My phone alone can do more than the computer can do," (P9, notes).

The current department policy on cell phones, DGO 10.07, was last revised in 1996. It does not address the use of cell phones by patrol officers, nor does it address the use of cell phones with advanced functionality. Indeed, the devices available today have functionality that would have been difficult to imagine in 1996.

Participants also discussed their use of non-department issued email accounts. Many participants, both those with and without department issued email accounts, indicated that they use non-department issued email accounts (meaning accounts not at the sfgov.org domain) for work email. As one participant said, "I hardly ever use the sfgov email. It's so

hard to get around. I mostly use an external, dedicated account," (P4, notes). The most common reasons for using third party email accounts were the poor usability of the Lotus Notes email client, limitations on file attachment size, and challenges accessing the sfgov email account from home. Several participants said they use non-department issued accounts at home to send themselves articles relevant to work at their sfgov accounts. Other participants described using non-department issued accounts to back up non-sensitive files or information for easy retrieval. One participant mentioned using a non-department issued account because a request for an sfgov account had not been filled, and an email account was required for work (P13, notes).

In every case, participants said that they are careful not to share sensitive information over non-sanctioned channels. Nevertheless, most participants indicated using at least one form of non-department issued communication.

Openness and Transparency

In the course of this research, I posed a hypothetical situation to the participants. It was very broad, and designed to evoke an emotional and exploratory response. The situation I posed was for participants to "imagine a website where a member of the public is able to search through and read email sent and received by all city employees. Some messages, and some parts of other messages, will be filtered out of this system to comply with the law, and will not be available to the public." From the ensuing discussion, I've identified three major themes. For the purposes of the following discussion, the system described in the hypothetical is referred to as an "open email" system.

Balancing public access with other interests

Every participant expressed a strong commitment to the public's right to information, but this was often balanced by a competing interest:

> "Transparency is important. The public is entitled to that. But you have to be able to operate the government safely and effectively. There must be an analysis under which the people's entitlement to be privy to the operation of their government comports with the safe and efficient operation of that government." *(P11, notes)*

Within the CPRA itself there are many exemptions, allowing for voluntary non-disclosure. Most participants were not familiar with the CPRA, so they were unable to comment on specific provisions. Nevertheless, there was an pervasive sense that public disclosure should be tempered by individual privacy rights, public safety, and the need for the government to be able to operate efficiently. There was, in many cases, something else as well. A sense that, while the public has a right to the information produced by and about the government, that perhaps they ought not to always exercise it. Said one participant, "If people need to see everything we're doing, they have too much time on their hands," (P5, notes). Another participant felt the tension more acutely:

> "Everybody can't have everything, but my gut feeling is that if there is a legal reason, an entitlement to access, then so be it. Otherwise, maybe everybody should just do their own jobs... However, there is absolutely no justification to hide things that need to be public, even if they're terrible. You have to sack up and own it." *(P11, notes)*

One participant attributed the tension expressed by many as a cultural norm, saying, "There's a culture in policing of being pretty careful who you tell what, sometimes to the point where it's pretty silly," (P2, notes). Another mentioned that within the department, a great deal of sensitive information is collected and shared, and that to minimize the potential for misuse, there is a policy of "right to know, need to know," (P3, notes). This policy serves as an internal guide and a formal policy that dictates who has access to what information. It is part of the policy that regulates access to criminal information databases, investigation files, and operational details, and was mentioned explicitly or alluded to by many of the participants.

Several participants also mentioned the privacy rights of the public as significant concerns in an "open email" system. One participant described how members of the public send reports of crimes to a shared SFPD email account, and worried that those emails would become public, exposing sensitive information, or merely by exposing potentially unfounded accusations against other members of the public (P8, notes).

Finally, there is a sense that the public should trust the police sometimes. The analogy one participant drew was to the use of firearms, "There has to be a certain amount of trust from the public. We're trusted to carry guns, which the public pays for, but I wouldn't let a member of the public hold my gun," (P13, notes).

Transparent email will lead to performative behavior

In addition to concerns about efficiency, public safety, and privacy, many participants expressed opinions about the way an open email system would change their use of email. A common sentiment was about stylistic changes, "I think it would make me more formal in my writing," (P2, notes), and some participants felt more self-conscious, "You definitely want to make sure you have spellcheck on. And what about people who don't have English as a first language?" (P5, notes). For some participants, the issue raised questions about their current use of email, "After six years, I'm pretty careful about what I say in emails, but not always," (P8, notes). Among all participants, there was a sense that "open email" would lead to more thoughtful, or more deliberate, use of email. As one participant said, "it reduces the freedom to be wrong" (P8, notes).

Latent in this finding is the Foucauldian sense of self-regulation in the face of pervasive sousveillance (Foucault, 1995). The potential for surveillance as a means of exerting power has been explored in the online space (Boyle, 1997) through a Foucauldian lens, but in these findings we see is potentially an inversion of the traditional dynamic. Rather than the state

exercising power through surveillance of the public, through the involuntary disclosure of communication that participants feel is relatively private, the public is able to exercise power through sousveillance. And as in Bentham's panopticon, those under observation consider action in line with the image they feel they are meant to portray.

Email would be used less

After expressing concerns about the potential harms of "open email" and thinking about new expressions of self-regulation, I encouraged participants to think about how such a system would effect their own use of email. Consistently, participants said that if there were an "open email" system, they would use email less. One typical response was to shift communication from email to another form of communication, "Definitely. I would use the phone more than send an email," (P6, notes). For some, this shift would clearly entail using a less efficient form of communication, "Email is so efficient, moving away would really slow us down," (P5, notes).

Several reasons for the decrease in use were cited. Some participants were concerned about the possibility of subordinates viewing their superiors' email in order to gain early information about transfers or position openings. Others saw the possibility of exhaustive email searches being used in retaliation in order to commit "organizational terror," (P2, notes). Another participant referred to the use of email in crafting new policies, and worried that "open email" would inhibit honest discussion. Many participants expressed concern for the privacy and safety of the officers themselves. Among these concerns was a fear that "personal information about officers contained in email could become public," (P5, notes), or that "infrastructure" (P3, notes) or "deployment information" (P8, notes) would become public.

Many of the concerns cited by participants for their projected decreased use of email if faced with an "open email" system are specifically allowed exemptions in the CPRA. However, even participants who were familiar at a high level with the CPRA were not familiar with the exemptions provided in the law. More surprisingly, nearly all participants felt that the "open email" system described in the hypothetical would change their behavior, yet even today the same material is available by request. This distinction can be understood as the difference between public information and published information.

Recommendations

The city of San Francisco and the SFPD face several challenges. These can be divided into three broad categories, with a discussion and set of recommendations in each. The three categories, broadly, are training for appropriate use of email, clear policies about the use of all available and currently used communication technologies, both department issued and non-department issued, and a thorough exploration of the risks and implication of an "open email" system.

Training

The current state of training for the appropriate use of email within the police department is limited. In part, this is likely due to the fact that virtually no patrol officers have email accounts (P1, notes), making training at the Police Academy less useful. In contrast, participants spoke favorably of the training they received, both at the Academy and throughout their careers, in other areas, including report writing (P13, P11, notes).

Because email has been introduced on an as-needed basis, users have developed a heterogeneous set of heuristics for determining when it is appropriate to share information over email, with whom, and with what degree of confidence in the confidentiality of their

messages. Many of these heuristics conflict with those developed by other members of the department, leading to a sense that "people have poor email etiquette," (P3, notes). More significantly, different standards negatively affect efficiency and reliability of the medium. As described above, participants who sit at the boundaries between email users and email non-users are forced to adopt hybrid communication models.

A further consideration for training is access to computing resources. Of the approximately 1,000 SFPD employees without email accounts today, many are patrol officers. I found that among this population, the lack of email was not felt as a negative. Instead, there is a sense that the work environment, both the physical environment and the pace, are not conducive to relying on email as a regular form of communication. The exception to this would be if patrol cars had convenient access to email (P9, notes). Without email in the patrol cars, patrol and beat officers have to use the shared computers terminals in the station. Since these computers are also used for report writing, they are valuable commodities (P7, notes). Currently, there are technical limitations that make email access from the MDCs infeasible. Most significantly, the mobile data service available in the patrol cars is not sufficient to support heavy email use across the network. However, if this barrier were addressed, the hardware could support either client based or browser based email (P12, notes).

As email is adopted in a wider array of roles within the department, the need for training will only increase. Since there is a significant population in the department without email, any training program would have to address both current and future employees, requiring both Academy and on-the-job training.

Policies

There is substantial confusion about what is acceptable use of non-department issued technology, as well as what best practices exist for the use of department issued technology. In GO 10.08 there is an instruction that SFPD employees are not to use department issued technology for personal use, but there is not a clear policy about using non-department issued technology for work. Even the instruction not to use department issued technology for personal use may not clearly articulate the privacy interests of individual employees sufficiently.

A recent case before the United States Supreme Court, *City of Ontario v Quon*, raised the question of a police officer's expectation of privacy in conducting personal communication using a department issued pager. While the policy and details in the case differ from the policies of the SFPD, the case raises important issues for every police department. Among the issues in the case is the question of where messages are stored (Volokh Conspiracy, 2010), what constitute appropriate grounds for an audit of an employee's messaging history, and what expectation of privacy an employee has when using a department issued communication device. The CPRA is brought to bear on some of these issues in the briefs submitted by both the plaintiffs and the defendants in the case, and those issues will be discussed below. However, the SFPD needs for clear policies, and clear articulation of those policies, for the appropriate use of department issued technology, beyond what is said in GO 10.08 d, which addresses misuse, rather than appropriate use.

While the department does have some policies about the use of department issued technology today, it has very little about the use of non-department issued technology. General Order 10.02 f.4 prohibits officers from carrying any items besides what is listed in the rest of 10.02 while on duty. General Order 10.07, which is not mentioned in 10.02,

indicates that "in order to improve the Department's communications capabilities, certain members are equipped with cellular telephones," but 10.07 does not address the use of non-department issued phones. However, through the interviews, it is clear that many patrol officers carry cell phones. Participants indicated that these devices are useful for communicating with colleagues and the public, interests acknowledged by the department in GO 10.07. However, the policy has not been updated to clarify the department's position on the use, or even the carrying, of these devices.

The department should issue clear policies about the appropriate use of non-department issued technology, as well as what the employees' expectation of privacy is on those devices. Additionally, as some participants indicated, phones today are capable of more than voice communication. They include GPS, email, internet access, MMS, and SMS. In the near future, mobile devices will likely include additional functionality. Whatever policies are adopted today need to address the broader context of use, and not focus on a single technology.

Open Email

The most challenging issue for the city and the SFPD to address is the development of an "open email" system. In addition to the findings discussed above, there has been significant work in the area of open government and transparency. While these topic, broadly, are not the focus of this paper[2], it is important to understand some of the challenges that other systems have faced, and the issues that have been raised in this area.

Today, email sent to and from city employees is potentially public through a CPRA request. A similar situation existed with court records in the before the last decade. While

[2] A comprehensive analysis of the transparency and privacy issues entailed by such a system will be provided another group on the CITRIS team, led by Joe Hall and Aaron Burstein.

records were available to the public upon request, essentially, they existed in "practical obscurity" (489 U. S. 749, 1989). Since then, court records have become widely available online, prompting a re-evaluation of dominant theories of privacy and the meaning of a public record. Several authors have suggested that the notion of privacy as synonymous with secrecy is no longer relevant (Solove, 2006; Barber, 2006, 2001; Nissembaum, 2004, 1998). Some authors cite specific harms that come from court records being made available en masse (Solove, 2001; Gottlieb, 2004; GAO Report, 2008; Opsahl, 2008), such as the disclosure of social security numbers, the aggregation of information, yielding a "data body" that is greater than the individual pieces of information disclosed, and unwanted marketing.

One of the challenges that arose in the digitization of court records was the fact that states, and even individual counties, handled the issue in very different ways. There was not a uniform approach. In 2002, the Conference of Chief Justices and the Conference of State Court Administrators produced a model policy for public access to court records that attempted to consider all the issues facing the courts and provide a set of guidelines and examples that courts could use in putting their records online. Considering the state of this process, as described in the Center for Democracy and Technology's 2002 report, "A Quiet Revolution in the Courts," such a model was sorely needed.

The judicial system has not been alone in facing challenges resulting from easy online access to electronic records. Some authors, and some participants in this study, have raised the issue of "naked transparency" (Lessig, 2009). The argument is that transparency without appropriate context invites misinterpretation. Lessig suggests that a member of the public with limited time and attention might see data appearing to show a correlation between campaign donations and a congressional voting record. Having discerned a pattern, the public assumes there is underlying truth and acts accordingly. But interpreting data requires

understanding the context in which it is produced, and the assumptions it embodies. Similarly, participants in this study worried that "Email is a record, but it's an incomplete record," (P8, notes).

In the face of these dangers, some have advanced the view that a document disclosed to one party need not be considered *absolutely* public. In this way, privacy, stripped of secrecy, is no longer a binary condition. Instead, privacy can be a function of context (Nissembaum, 2004). In this model, the courts, or indeed any public agency, might grant access to public documents to an individual, but deny them to a data aggregator. [3]

The biggest challenge faced by an "open email" system, as with the electronic court records, is that automated filtering is hard. The courts are still having problems with un-redacted social security numbers, and they deal with a relatively limited set of documents. The problem for an automatically filtered, push-publication email system is that the list of exemptions provided by the CPRA, and the very issues that participants expressed concerns about, require a high level of understanding of the content of communication, as well as its structural features. While a certain amount of role based filtering, for example emails sent to or from an attorney, is possible, tailoring these filters so they are neither overly protective or liberal will be very challenging. A system that is too conservative will not, ultimately, reduce the number of formal CPRA requests made to the city, a stated goal of the "open email" proposal. However, a system that is too liberal in disclosing sensitive material will push users to other communication media, and will reduce the efficiency of the SFPD while providing no benefit of openness to the public. On top of the technical challenge, there is a challenge in showing users that their expectations and the filters built into the system are in alignment.

[3] This paper does not explore the legal implications of this decision.

A commonly expressed sentiment among the participants is that without knowing exactly what would be filtered, the participants would err on the side of not using email at all.

The participants in this study demonstrated an implicit understanding of the distinction between potentially public documents and actually published documents. Their reticence to communicate in a system embracing the push-publication model, an "open email" system, is supported by the challenges faced by the court system.

Overcoming the technical and social challenges to an "open email" system might be possible, but would require embracing an alternative model for privacy. Such a model would require looking not only at what constitutes a public record, but at who can and should have access to each of those records. It is possible that this additional consideration is not supported by the law, although some authors have considered the question (Solove, 2002) and posited that this model may be compatible with open government laws, like the CPRA.

Conclusion

As the volume of data produced increases, there's a corresponding impulse to create better, faster tools for consuming and processing it. But it is ultimately people, both producing and consuming, the information, and it is the human implications that are most important on both sides.

The city of San Francisco and the SFPD have a great challenge, and a great opportunity, in creating a unified, open email system. Considering that today the police department only has email accounts for about 60% of its employees, it is risky to radically alter the system before establishing accounts, and patterns of use, for the remaining 40%. It is clear from this research that the existing use of email varies widely across the department, and there has been little work done to clarify the appropriate role of email as a communication medium.

The participants in this research shared their concerns about the prospect of an open email system, but acknowledged the public interest in seeing how those in government conduct their work. As more communication takes place in media not imagined when the CPRA and similar laws were passed, it is important for the public to continue having access and insight into the business of government. Most of the challenges explored in this paper are not, fundamentally, about limiting public access to government information. They are, instead, challenges that require human decision making and discretion before any technological systems can be implemented. The danger presented by open email is simply that email is something that happens on the computer, and therefore the temptation is to treat it as a technological system, rather than as a socio-technical system. As long as the focus remains on the people involved, rather than the specific technologies, the interests of both the SFPD and the public's access to government information can be advanced.

Acknowledgement and Thanks

This project would not have been possible without the work and support of my advisor, Deirdre Mulligan, and the Samuelson Law Clinic team members, Shahrzad Radbod and Lin Tzeng. I was lucky to work with Lt. Greg Yee of the SFPD and all of the members of the SFPD who participated in this study. Finally, thank you to Katherine, for your tireless support and keen mind.

Appendix 1: Request For Quote

Request for Quote

The Department of Technology for the City & County of San Francisco is requesting a quote for the analysis and compilation of business, technical and policy requirements, for the migration from IBM's Lotus Notes to Hosted MS Exchange email environment.

The awarded Contractor will meet with each of the Cities departments to gather business, technical and related policy requirements and to document each of the city departments needs. The information gathered will be used as the basis for writing a formal RFP that will be used to procure services for a hosted Microsoft Exchange environment.

- Desired start time for the project is immediate, to run approximately 3-4 months
- Quotes should be on a time and materials basis
- All quotes must be submitted no later than 5:00pm, Friday, December 11, 2009
- All questions should be addressed to: Kendall Gary at kendall.gary@sfgov.org
- Submission format: Email to Kendall Gary – kendall.gary@sfgov.org
- Submit resumes for candidate(s) for this position.

The contractor must have experience in developing and architecting enterprise solutions for public sector, as well as expert knowledge in all aspects of email features, email security and public policy.

Items that will need to be addressed include:

- If departments have an Active Directory structure in place, is it a model that can directly connect to the City's ADFS
- To be consistent with the direction of The City & County of San Francisco, to be an open and transparent organization, the contractor will need to help define and evaluate the policy and technical implications of "open email".
- Case study of Law Enforcement Agency email pilot project.
- Each department's legal requirement(s) for email retention, storage and archival.
- Evaluation of any specific feature sets of email. Obtaining any unique requirement that would be needed.
  - instant messaging,
  - Need for hand-held mobile devices or smart phones,
  - anti-spam and anti-virus functionality
  - etc.
- Security and/or regulatory requirements including encryption needs
- Storage capacity requirements for each person in a department.
- Roles and responsibility for departmental Administrators.
- Recommendation for the maintenance and structured of email domain names across departments.
- E-Discovery and forensic features and capabilities for departments and basis.
- Prepare procedures documentation; generate reports and statistics, design tables, prepare flow charts and other graphic presentations.
- Disaster and business continuity recovery requirements
- Back-up requirements

End of Document

References

Books, Articles, and Law

Babchuk, W. A. n.d. "Grounded Theory 101: Strategies for Research and Practice." in Proceedings of the 28th Annual Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education. Chicago: Northeastern Illinois University.

Barber, Grayson. 2006. "Personal Information in Government Records: Protecting the Public Interest in Privacy." *Saint Louis University Public Law Review* 25:63.

Barber, Grayson. 2001. "Uneasy Access: Court Records Online." *New Jersey Law Journal* 163.

Blanchette, J. F, and D. G Johnson. 2002. "Data retention and the panoptic society: The social benefits of forgetfulness." *The Information Society* 18:33–45.

Boyle, James. 1997. "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors." *University of Cincinnati Law Review* 66:177.

Charmaz, K. 2005. *Grounded theory : Methods for the 21st century*. London ;Thousand Oaks Calif: SAGE Publications.

Cohen, Julie E. 2008. "Privacy, Visibility, Transparency, and Exposure." *University of Chicago Law Review* 75:181.

DOJ v. Reporters Comm. For Free Press, 489 U. S. 749 (1989)

Foucault, Michel. 1995. Discipline and punish : the birth of the prison. 2nd ed. New York: Vintage Books.

Fu, Helen. 2010. "When public records are less than public: How governments try to use copyright to limit access to data » Nieman Journalism Lab." http://www.niemanlab.org/2010/04/when-public-records-are-less-than-public-how-governments-try-to-use-copyright-to-limit-access-to-data/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+NiemanJournalismLab+%28Nieman+Journalism+Lab%29 (Accessed May 2, 2010).

Fung, Archon, Mary Graham, David Weil, and Elena Fagotto. 2004. "The Political Economy of Transparency: What Makes Disclosure Policies Sustainable?." *SSRN eLibrary*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=384922 (Accessed May 2, 2010).

Gottlieb, K. 2004. "Using court record information for marketing in the United States: It's public information, what's the problem." in an International Workshop on WHOLES—A Multiple View of Individual Privacy in a Networked World, Swedish Institute of Computer Science, Sigtuna, Sweden. http://www. privacyrights. org/ar/courtmarketing. htm (accessed July 13, 2004).

Kohn, Margaret. 2006. "From Citizen to Subject: The Perils of Privacy." UC Berkeley http://www.law.berkeley.edu/institutes/bclt/events/unblinking/unblinking/kohn_paper.pdf.

Lessig, Lawrence. 2009. "Against Transparency | The New Republic." http://www.tnr.com/article/books-and-arts/against-transparency (Accessed May 2, 2010).

Mousavi, N., and others. 2005. "When the Public does not Have a Right to Know: How the California Public Records Act is Deterring Bioscience Research and Development." *Duke L. & Tech. Rev.* 2005:23–26.

Newsom, Gavin. 2009. "ED 09-06 Open Data." http://www.sfmayor.org/wp-content/uploads/2009/10/ED-09-06-Open-Data.pdf (Accessed May 2, 2010).

Nissenbaum, H. 2004. "Privacy as contextual integrity." *Wash. L. Rev.* 79:119.

Nissenbaum, H. 1998. "Protecting privacy in an information age: The problem of privacy in public." *Law and Philosophy* 17:559–596.

Nissenbaum, Helen. 1994. "Computing and accountability." *Commun. ACM* 37:72-80.

Opsahl, Andy. 2008. "Privacy: Agencies Struggle to Redact Personal Data from Online Public Documents." http://www.govtech.com/gt/375540 (Accessed May 2, 2010).

Sklansky, D. A. 2005. "Police and democracy." *Mich. L. Rev.* 103:1699–2209.

Solove, Daniel. 2006. *Information privacy law*. 2nd ed. New York NY: Aspen Publishers.

Solove, Daniel J. 2001. "Access and Aggregation: Public Records, Privacy and the Constitution." *Minnesota Law Review* 86:1137.

Sudbeck, Lynn E. 2006. "Placing Court Records Online: Balancing Judicial Accountability with Public Trust and Confidence: An Analysis of State Court Electronic Access Policies and a Proposal for South Dakota Court Records." *South Dakota Law Review* 51:81.

Surden, Harry. 2007. "Structural Rights in Privacy." *SMU Law Review* 60:1605.

Swire, P. P. 2004. "Model for When Disclosure Helps Security: What Is Different about Computer and Network Security, A." *J. on Telecomm. & High Tech. L.* 3:163.

Winn, Peter A. n.d. "Judicial Information Management in an Electronic Age: Old Standards, New Challenges." *SSRN eLibrary*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1438674 (Accessed May 2, 2010).

Websites

"- official website of THE LOS ANGELES POLICE DEPARTMENT." http://www.lapdonline.org/home/content_basic_view/36329 (Accessed May 2, 2010).

"A Quiet Revolution in the Courts: Electronic Access to State Court Records." http://74.125.155.132/search?q=cache:http://opt-out.cdt.org/publications/020821courtrecords.shtml (Accessed May 2, 2010).

"Access to Records : First Amendment Coalition." http://www.firstamendmentcoalition.org/category/resources/access-to-records/ (Accessed May 2, 2010).

"ACLU of Northern California : Frequently Asked Questions about Copley Press and SB 1019." http://www.aclunc.org/issues/criminal_justice/police_practices/frequently_asked_questions_about_copley_press_and_sb_1019.shtml#1 (Accessed May 2, 2010).

"CA Codes (gov:6250-6270)." http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270 (Accessed May 2, 2010).

"California Constitution - Article 1." http://www.leginfo.ca.gov/.const/.article_1 (Accessed May 2, 2010).

"City & County of SF Information Related to the American Recovery and Reinvestment Act of 2009." http://recoverysf.org/intranet/RecoverySF/ (Accessed May 2, 2010).

"DataSF - Liberating City Data." http://www.datasf.org/ (Accessed May 2, 2010).

"GAO-08-1009R, Social Security Numbers Are Widely Available in Bulk and Online Records, but Changes to Enhance Security Are Occurring." 2008. http://www.gao.gov/htext/d081009r.html (Accessed May 7, 2010).

"Mobile phones connect police, community | San Francisco Examiner." http://www.sfexaminer.com/local/Mobile-connects-police-community-59697032.html (Accessed May 6, 2010).

"Open Government Initiative | The White House." http://www.whitehouse.gov/open (Accessed May 2, 2010).

"Privacy and Information Quality." http://it.ojp.gov/default.aspx?area=globalJustice&page=1238 (Accessed May 2, 2010).

"Prop 59 : First Amendment Coalition." http://www.firstamendmentcoalition.org/category/resources/prop-59/ (Accessed May 2, 2010).

"San Francisco Police Department : SF Police General Orders." http://sf-police.org/index.aspx?page=1720 (Accessed May 2, 2010).

2009. "San Francisco, the city that's open for data | Technology | The Guardian." http://www.guardian.co.uk/technology/2009/oct/14/san-francisco-open-city-data (Accessed May 2, 2010).

"The Volokh Conspiracy » Was the Stored Communications Act Actually Violated in City of Ontario v. Quon?." http://volokh.com/2010/04/19/was-the-stored-communications-act-actually-violated-in-city-of-ontario-v-quon/ (Accessed May 2, 2010).

"Transparency and Open Government | The White House." http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/ (Accessed May 2, 2010).

"What is PACER?." http://pacer.uscourts.gov/pacerdesc.html (Accessed May 2, 2010).