Timothy H. Edgar

Watson Institute for International Studies

Brown University

"Data Security at the Postal Service"

Testimony at a hearing before the

United States House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Federal Workforce, U.S. Postal Service and the Census

Wednesday, November 19, 2014

Chairman Farenthold, Representative Lynch and members of the Subcommittee,

Thank you for this opportunity to testify on questions that implicate the privacy of the mail.

I served in the Obama White House as the first privacy and civil liberties official for the National Security Council, focusing on cybersecurity. Under President Bush, I was the deputy for civil liberties for the Director of National Intelligence. From 2001 to 2006, I was the national security counsel for the American Civil Liberties

Union. I am currently a visiting fellow at Brown University's Watson Institute for International Studies, where my work focuses on the policy challenges posed by reconciling security interests with privacy and civil liberties.

"Is Nothing Sacred?"

"Is nothing sacred?" has been the most common reaction of friends and colleagues to the news about privacy problems at the United States Postal Service (USPS). The dismay says a lot about the trust that Americans place in the post office to protect the privacy of their correspondence. We know the NSA collects telephone call detail records, Internet metadata and electronic communications. Major technology companies, such as Google and Facebook, routinely monitor their users to deliver targeted advertising. The post office seemed to offer a last refuge for American privacy. It is indeed alarming that the government is capable of invading our privacy even if we choose to live our lives as complete technophobes, without ever touching a phone or a computer.

The subject of today's hearing is not the opening of mail, which requires a warrant, but the investigative tool known as "mail covers." Mail covers involve copying what appears on the front and back of an item of mail – generally, addresses for a sealed envelope or the contents of postcards or pamphlets. When properly controlled, the tool is an appropriate one for law enforcement and national security investigations, but it carries much the same privacy risks as orders for communications metadata.

Monitoring of mail through mail covers can give the government a revealing picture of a person's life, including who among their friends and relatives is thoughtful enough to send a traditional letter or card, the accounts they maintain at banks and other financial institutions, and the organizations on whose mailing lists they belong. Mail monitoring will also reveal connections with physician's offices, which can reveal very intimate information. The name and address of such correspondence can reveal that a person has a condition that requires a specialist, is seeing a psychotherapist, or has obtained an abortion or family planning services. Physicians often rely on the mail to meet federal privacy requirements precisely because Internet communications are usually unencrypted and therefore insecure.

Unfortunately, the Inspector General of the USPS has found major problems in how the postal service is handling these requests. The USPS authorized 49,000 mail covers in the past fiscal year, a much higher yearly figure than it had previously disclosed in response to Freedom of Information Act requests. The Inspector General's report found that 20% of such mail covers lack the required written authorization. 13% did not include sufficient justification and yet these requests were still granted. The systems for keeping track of mail covers were also faulty. In almost a thousand cases, monitoring continued even after requests had expired.[1]

These findings represent more than a few compliance problems at a large federal agency. They shake our confidence in longstanding principles of privacy and civil

liberties that have been a part of the American system since the days of George Washington.

The Privacy of the Mail: Constitutional Origins

The federal constitution gives the Congress the power "To establish Post Offices and post Roads." In 1792, Congress passed, and George Washington signed, the first permanent law establishing the federal postal service. In that law, Congress flatly prohibited the opening of federal mail. It was a departure from the practices of European governments, who had long maintained secret rooms for monitoring correspondence. In France at the time of the revolution, the room was known as the *cabinet noir* – the "black chamber" – and it was a hated instrument of oppression. The 1792 postal service law would ensure that no such institution would be established in the United States. For more than a century and a half, the privacy of the mail was generally respected, even as newer forms of communication, such as telegraphs, came under broad wartime surveillance, beginning during the presidency of Abraham Lincoln.[2]

In what appears to be the first case interpreting the Fourth Amendment, the Supreme Court reaffirmed the privacy of the mail. In the 1878 case of *Ex Parte Jackson*, the Supreme Court wrote, "Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in

their own domiciles."[3] The Supreme Court's message was clear – the right of privacy in personal correspondence was no less important than a citizen's right to privacy in his home. In both circumstances, a warrant would be required for the government to conduct a search.

Of course, *Ex Parte Jackson* also made clear that this level of protection extended only to sealed correspondence. The "outward form" was exposed to view and therefore not protected by the warrant requirement. The practice of "mail covers" evolved from this distinction. Mail covers allow police and other investigators to track with whom someone is corresponding, without the need to obtain a warrant. It served – and still serves – the same purposes as orders for telephone and Internet metadata today. Indeed, the distinction between the inside and outside of sealed letters and packages provides the basis for the distinction between content and metadata that is crucial to the Fourth Amendment analysis of all forms of communication.[4]

Monitoring the Mail: Cold War Abuses

Between 1940 and 1973, the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) engaged in twelve separate illegal mail monitoring programs. It began with a wartime program to open mail of Axis diplomatic establishments. In 1940, the British taught the FBI what the 1792 law had outlawed: how to secretly open mail. After the war, the government engaged in

much more widespread mail monitoring of ordinary Americans that included both mail covers and illegal mail openings.[5]

The largest of these programs was codenamed HTLINGUAL. It was a CIA program that ran from 1953 to 1973, targeting all correspondence to and from the Soviet Union. This program was run out of New York, where most letters left or arrived. The CIA proposed it as a "mail covers" program and obtained the postal service's cooperation on that basis. Arthur Summerfield, the Postmaster General, approved the program in 1954, but it appears he never approved opening of mail. In fact, while 215,820 letters were illegally opened, a much larger number – 2.7 million – were photographed, front and back. The monitoring of the outside of mail was therefore more than ten times larger in volume than CIA's illegal opening of sealed mail. The record is unclear as to whether any subsequent Postmaster General was advised that mail was actually being opened; care seems to have been taken to allow the postal service to be able to deny, at least officially, knowledge of this aspect of the program.[6]

Mail was intercepted first at LaGuardia Airport, then at Idlewild (later Kennedy) Airport by a postal clerk. The clerk received a very sizeable annual bonus of $500 from the CIA for his cooperation. Mail was delivered to a team of CIA agents in a secret room. They processed 5,000 to 15,000 items of daily correspondence, photographing as many items as possible. A much smaller number – 35 to 75 letters – were surreptitiously selected ("swiped" was the term used by the agents) for later

opening at the CIA's Manhattan Field Office. Each agent who opened mail attended a one-week course called "flaps and seals" at CIA headquarters. The method was simple – the letters were opened using the steam from a kettle and a narrow stick. The CIA attempted to improve the process with a special steam oven capable of handling one hundred letters at a time, but it never worked properly, so agents went back to the tried-and-true steam kettle method.[7]

Agents involved in the program were not foreign intelligence experts and much of the selection was essentially random. Agents were given little guidance on which letters to open, beyond memorizing a "watch list" of persons and organizations of interest, including peace groups such as the American Friends Service Committee, authors including Edward Albee and John Steinbeck, publishing companies, and at least one member of the Rockefeller family. Most of the mail selected was not based on the list. One agent testified that mail was selected "according to individual taste, if you will, your own reading about current events. . . . We would try to get a smattering of everything, maybe the academic field or travel agencies or something." The result of the program was monitoring of Americans for domestic purposes, not foreign intelligence. Over the life of the program, 57,846 items of correspondence were disseminated by the CIA to the FBI.[8]

Despite grand plans for uncovering spies, developing agents inside the Soviet Union, and obtaining valuable foreign intelligence, the record shows that HTLINGUAL's value was doubtful. CIA officials deemed the material "of very little value," describing the

intelligence as "meager." By the early 1970's, it had become clear that the program – which officials had always understood was illegal – could create real embarrassment for the CIA and the FBI. It was terminated in 1973, shortly before these and many other Cold War abuses were investigated by a select committee lead by Senator Frank Church.[9]

While the CIA and FBI were directly responsible for the illegal monitoring of mail during these years of Cold War surveillance excesses, the postal service was also to blame. Its officials cooperated with the program. During the initial stages of the program, postal employees were present as the CIA photographed the outside of mail, apparently looking the other way as some letters were "swiped" by the agents. Later, they gave the CIA a separate room where they were left, unmonitored, with sacks of private letters. They knew or at least had strong reason to suspect that the opening of mail was the likely purpose of the program and that it was a crime if done without a warrant. The postal service, and the Postmasters General who knew of the program, did little to raise these legal concerns within successive administrations. The result was monitoring of academics, journalists, innocent travelers and many others – in short, widespread abuse of the rights of Americans.

Lessons for Today

The Inspector General's report of May 2014 on mail covers does not involve anything on the scale of the illegal mail monitoring uncovered by the Church

Committee, but it is very troubling nonetheless. First, the number of mail covers provided to outside agencies, at 49,000 over the course of the past fiscal year, is well in excess of what had been understood based on the postal service's response to Freedom of Information Act (FOIA) requests. Previous estimates were on the order of 8,000 per year. The discrepancy seems to be the result of the postal service's decision to limit its FOIA responses to law enforcement requests, excluding national security requests and mail covers ordered by its own inspection service. The USPS even attempted to keep this Inspector General report secret.[10] The higher number is troubling in itself. The lack of transparency shown by the postal service is more troubling.

The compliance incident rate found by the Inspector General – 20% of mail covers approved improperly because of a lack of written authorization, and 13% approved without sufficient justification – are likewise not acceptable. By way of contrast, the National Security Agency (NSA), whose compliance missteps have garnered far louder condemnation, has carefully tracked compliance incidents under new Foreign Intelligence Surveillance Act (FISA) authorities. According to a declassified assessment by the Department of Justice and the Office of the Director of National Intelligence, the compliance incident rate – the percent of improperly targeted selectors – for 2013 is less than one half of one percent.[11] At least when it comes to compliance, it appears that the USPS has done a far worse job of protecting privacy than the NSA – not what the public might have expected.

As the mail monitoring abuses of the past have demonstrated, vigilance by the postal service is necessary to protecting the rights of the public. The postal service must be a stickler for proper procedure – it cannot afford to be lax, especially when it comes to investigative tools, like mail covers, that require no judicial review or oversight. The USPS should stand for the rights of its customers when it comes to their privacy. Just as customers expect companies like Verizon and Google to insist on proper legal authorization for government data requests, postal customers should expect the same.

The USPS can learn important lessons not only from past abuses involving mail monitoring, but from the actions of the government and industry in responding to recent surveillance controversies. Like the NSA, the USPS can adopt much more rigorous and detailed oversight of its handling of privacy requirements. Like Google and other technology companies, the USPS can publish periodic transparency reports detailing how many mail covers and warrants it processes each year, under what authorities, and how it addresses improper requests. The USPS should fight to make more, not less, information available about national security requests. The DNI is now providing yearly aggregate information about many such requests under national security authorities involving electronic surveillance; there is no reason such information should be withheld when it comes to monitoring the mail.[12]

Finally, the USPS must be careful to avoid the problems created by the NSA's bulk collection of telephone metadata. The system for monitoring the outside of mail

takes advantage of new imaging software that photographs every letter processed by the USPS. This system effectively facilitates a form of bulk collection of postal metadata. While the USPS requires individual suspicion before it approves release of this metadata as part of its mail covers program to requesting state and federal agencies, the existence of the database raises major security and privacy questions.[13] Congress should scrutinize whether this database is necessary or whether less intrusive alternatives exist, what protections ensure against hacking into the database, how long the data is retained, and who has access to the data. Congress has been debating the NSA's bulk collection of telephone metadata for well over a year. It should ask the same questions of the USPS about this imaging software.

Conclusion

The United States Postal Service is a venerable and trusted institution, with roots going back to the beginning of the republic. History shows, however, that the USPS has not always lived up to the ideals of the nation, or its own ideals, in vigorously protecting the privacy of the mail. These failures were not the result of malice, but of laxity in enforcing privacy requirements. Enforcing these requirements to the letter is the best safeguard against future abuses.

---

[1] Office of Inspector General, United States Postal Service, "Postal Inspection Mail Covers Program (Audit Report)," May 28, 2014.

[2] Ralph E. Weber, Masked Dispatches: Cryptograms and Cryptology in American History, 1775-1900, at 49-50 (2013); David Kahn, *Back When Spies Played by the Rules* (op-ed), N.Y. Times, Jan. 13, 2006.
[3] *Ex Parte Jackson*, 96 U.S. 727, 733 (1878).
[4] Orin S. Kerr, *Apply the Fourth Amendment to the Internet: A General Approach*, 62 Stanford Law Rev. 1005, 1009-10, 1022-23 (2010).
[5] Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, Vol. 3, 94th Cong., 2d Sess., Rep. No. 94-755 (April 23, 1976) at 561-67.
[6] *Id.* at 567-610.
[7] *Id.*
[8] *Id.* at 574-75, 632.
[9] *Id.* at 567-610.
[10] Ron Nixon, *Report Reveals Wider Tracking of Mail in U.S.*, N.Y. Times, Oct. 27, 2014; Josh Gerstein, *Snail mail snooping safeguards not followed*, Politico, June 19, 2014.
[11] Semiannual Assessment of Compliance for FISA § 702, June 1, 2012-Nov. 30, 2012 reporting period, at 23 (August 2013), available at http://icontherecord.tumblr.com/post/58948476651/additional-declassified-documents-relating-to
[12] Office of the Director of National Intelligence, 2013 Transparency Report (June 26, 2014), available at http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013
[13] *See* Nixon, *supra* note 10.