2013-2014 MONTEREY COUNTY CIVIL GRAND JURY

INTERIM FINAL REPORT NO. 5

PRIVACY AND SECURITY OF COUNTY ON-LINE

DATA AND INFORMATION SYSTEMS

PRIVACY AND SECURITY OF COUNTY ON-LINE

DATA AND INFORMATION SYSTEMS

SUMMARY

The impetus for the Civil Grand Jury (CGJ) to investigate Monterey County Information Technology operations, concerning its obligation to protect County controlled and stored data, was a September 2013 press release from the Monterey County Department of Social Services. This press release disclosed for the first time that a data breach, by persons unknown, had occurred in March 2013 on an old 2008 computer health database connected to a California State network, which data was illegally accessed through State computers. After reviewing the facts, the CGJ concluded that this was an unusual event, the exact nature of which was unlikely to occur again, the data was very old, and the Social Services Department had appropriately notified the victims -- albeit not as rapidly as contemplated by the Privacy laws existing at the time.

However, in the process of investigating this reported breach, the CGJ determined that the County Policies and Procedures for protecting data on Monterey County computer systems were totally obsolete and unlikely to be in compliance with existing Privacy and Data Protection laws and regulations. As a result the CGJ commenced in depth interviews with various County departments and personnel, during which it became clear that efforts before and during the 4th quarter of 2013 to update and replace 2008-age Privacy Policies and Procedures were not progressing well. It was also evident that major operational changes were needed to bring the County into compliance with such laws.

Insufficient funding resources, bureaucratic inertia, changes in management of the IT Department and, more recently, other priorities by the County Counsel's office had caused the Policy revision process to drag on for many years. During the past several years the IT Department and its new Director have been acutely aware of this situation but were unable to move the matter along at an adequate and desirable pace until very recently.

There was also an apparent lack of realization by many County officials that a number of new and different Privacy laws and Data Breach Notice requirements applicable to Monterey County, to be effective January 1, 2014, required immediate completion of the long delayed County Privacy and Security policies revisions. Generally, these new laws relate to notices of breach and use of "Personally Identifiable Information" ("PII"). See the listing of the new California Privacy laws at the California Attorney General's website, http://oag.ca.gov/privacy/privacy-legislation/leg2013.

To their credit, when this was called to County officials' attention by the CGJ, action was promptly taken to commence completion of the policy updating. However, this was not completed until May 2014 because of the complexity of such revisions and the need for all key County departments to participate in the updating process. These new Policies were approved by the Board of Supervisors in May 2014, yet major efforts will still have to be made so that said policies are properly implemented and well understood by County staff. The required new technical software must also be installed, become operational, and then used properly.

However, even with the adoption of these new Policies and new technical steps to protect the data, the CGJ concludes that the County should provide more funding for continuing legal and technical education for its staff to be in full compliance with these important laws in the future. This would help the County avoid serious penalties and potentially expensive litigation in case of data breaches or other failure to comply with these laws. Proper and constant on-going legal review must be scheduled, and the proposed new operational procedures must be implemented.

As a result, the CGJ felt it necessary to compile a detailed series of Factual Conclusions and Recommendations, all set forth below, which are aimed at helping the County and the public to understand why these admittedly costly steps ***must*** be taken by the County. In some ways, these recommendations might be thought of as a form of liability insurance against events over which the County does not have much control – like earthquakes or floods. The cost of failure to comply can run into the millions of dollars, per event, as recent commercial data breaches, like that of the Target Stores, have shown.

INVESTIGATIVE METHODOLOGY

During this investigation the CGJ interviewed key personnel of the following Offices and Departments concerning the Privacy and Data Security processes in Monterey County government operations:

1. Several members of The Board of Supervisors
2. Department of Information Technology
3. Offices of the County Counsel
4. Department of Health and Social Services
5. Chief Administrative Officer of the County, and his two Deputies
6. Treasurer-Tax Collector
7. Offices of the District Attorney

The CGJ also spoke with several well-known authors of published legal materials on the subject of Privacy and Security, and conducted extensive research on the subject on the Internet. For further background, some members of the CGJ read and reviewed a 150 page publication entitled "Foundations of Information Privacy and Data Protection," and several similar books and program materials sponsored by the International Association of Privacy Professionals ("IAPP").

IAPP. IAPP is an internationally recognized group of over 22,500 individuals and sponsoring corporations that conduct seminars and educational programs, including the publishing of books and instructional materials on the subject. One Grand Juror even enrolled in and attended an IAPP introductory class, at his own expense, to gain a better understanding of these issues.

In the investigative process, some members of the CGJ spent significant time reading and reviewing the immense body of laws, rules and regulations promulgated by Federal, State and foreign governments in this area of the law, including the excellent website of the California Attorney General at www.oag.ca.gov/privacy. This is an excellent starting point for such an inquiry.

As the California AG states there:

> "In the 21st century, we share and store our most sensitive personal information on phones, computers and even in 'the Cloud'. Today more than ever, a strong privacy program is essential to the safety and welfare of the people of California and to our economy."

The CGJ believes this is an accurate summary of the current environment for data stored and used by all businesses and government agencies, including Monterey County government. More attention to this area of the law by our County government is imperative.

BACKGROUND

How We Got Here.

It may help to review briefly how we as a society got from "the old ways" to the Information Age. Prior to the extensive use of computers and the Internet, to get cash we usually went to our local bank where we presented our check or withdrawal slip to the bank teller, who probably knew us personally, or at least could check on a ledger card next to his station to see what our signature looked like and what our bank account balance was. We were handed the cash and left, after thanking the teller personally. There were no ATM's and the Internet was just an idea under consideration by futurists.

Today we can deposit checks using our cell phones, pay our bills on line, and make purchases from merchants across the country for amounts running into the thousands of dollars by merely typing in a credit or debit card number, a name, a PIN or other identifying password, and then hitting the Return or Enter key. Funds are transferred and the transaction completed instantly. Our bank can be in New York or France, and we as customer/residents of Monterey County could be traveling in Asia at the time. This worked well until the Internet made international commerce so simple that international cybercrime became equally simple. Thieves thrive on invisibility, the complexity of efforts to trace them, and speed and distance.

Now we are faced with a situation where vast sums of money and information about a customer/user can be captured and later used to create millions of fraudulent transactions, unless the computer system accessed and the means of downloading these identifying pieces of data employ complex protective software that quickly warns of intrusion. This environment makes it clear that even with sufficient validation identification in the form of a name, credit card number and password, the user is still at the mercy of the security systems used by our distant electronic merchants. The same problem exists on government systems that collect or use information from its citizens.

What These Laws Are and Do.

To recognize this new disparity of control, hundreds of laws have been passed at all levels aimed at protecting the customers and users from the theft of data and information. As thieves become more adept and systems become more complex, the protective laws have to become more complex. In fact today there are, just in the US and its 50 states, at least 29 separate bodies of such laws. These laws often change annually, and become broader in scope with each change. These rapid changes mean that constant legal and technical help and continuous review of databases, websites, statutory notices, and contracts is required. These protective costs cannot be avoided because of the pervasive nature of these laws.

Notably, these laws make a distinction between "data" and "information." The difference is that a single piece of *data* or list of data, say credit card numbers, has little value to a criminal, *but* when linked to a name, email address, or PIN number it becomes highly useful *information* which, in combination, can be used to steal money or create illegal transactions or transfers of money. This is why such combined data is called Personally Identifiable Information or "PII" in the lingo of these laws.

These expansive laws take two forms:

> *Privacy Protection* laws which impose on the government agency, hospital or merchant an obligation to use "reasonable care" in protecting the data collected and used, *and* of advising customers and citizens what use is being made of data collected from them and why. Thus, for example, the required Privacy notices on webpages are very important. Coincidentally, the notices on the current Monterey County website appear to be non-conforming as of the date of issuance of this Report.
>
> *Breach Notification* laws are the other form of legislation that impose a very expensive obligation on the merchant or government agency to notify the customer or citizen if the Privacy Protection failed and the data system is breached. Experts in this field tell us that the average cost of just the notification and remediation steps, *per customer or citizen,* is

$188, even before customer or user damage claims are dealt with. Significantly, the total cost of notifying the owners of the 140,000 records of Monterey County residents of the 2013 breach, described at the outset of this Report, was estimated by a County manager to be over $87,000, including staff time and mailing costs.

Why Monterey County Has to Comply.

While these laws are incredibly complex and change yearly, Monterey County has no choice but to comply because many such laws impose financial penalties on entities that are not in compliance. In the event of a breach where the entity is held not to have used reasonable care in attempting to protect the data, statutory penalties can be up to $150,000 for each event, and there are already cases where the total penalties have run into many millions of dollars. Such failures to protect the data can also be the basis for private class actions, thereby risking millions of dollars in legal fees and damages.

The California Breach Notification law expressly applies to counties and other local agencies, as of January 1, 2014, whereas it previously applied only to state agencies. In most cases the obligations imposed by these breach and notice requirements can only be ascertained by qualified legal counsel. Thus, County Department heads and County Counsel must work together, quickly, to determine what changes may be required, each time a law or regulation is changed or passed.

How Does Monterey County Comply and How Does The Process Work?

It is important to understand that compliance is a two-fold process where County IT security experts must handle the IT hardware and software compliance side of things, while the legal experts must determine both the reasonableness of the technical compliance *and* must provide the language for notices and in any third party providers' contracts and licenses. Neither is a simple task, and the personnel assigned to the task must be carefully trained and must remain aware of the constant changes in these requirements. These advisors cannot fall behind in their knowledge of these laws without increasing financial and legal risks to the County.

Even more difficult is the fact that every time a contract, a website section, or a procedure or policy is changed, adopted or instituted, both the technical and the legal professionals must be made aware of the change or the event. For this reason, nearly all County personnel of every department must be aware of the existence of these laws and requirements. This is especially so since virtually every County employee has or uses computers, cell phones, tablets, or other devices which are connected to the Internet and susceptible to intrusion by cyber thieves. No amount of training and technical help will ever *totally* prevent intrusions or loss of information, but this constant effort has to be made to comply with the law and to protect County residents and their County government.

FINDINGS

F1. During the past eight or more years the Monterey County government has not devoted adequate attention to compliance with the California and Federal Privacy laws, and must now immediately change this attitude to strict attention and compliance, if it is to avoid serious financial consequences for potential violations.

F2. The present old and defective Privacy and Data Breach Notification Policies are to be replaced immediately and the newly developed 2014 versions disseminated promptly to all Department heads now that they have been approved by the Board of Supervisors. This must be quickly followed-up by education of all County employees as to these new rules, and the appropriate conduct required when using or operating County IT and communication systems.

F3. County Counsel's office has not been adequately aware of these Privacy issues in the past, in part because of inadequate staffing and education of its lawyers, but it is now actively trying to change this situation within its budget limitations. However, it clearly needs additional funding to address these issues and to assist the IT Department and other County departments with this complex area of the law.

F4. The County IT Department needs to continue its active pursuit of software and hardware means of preventing intrusions, and to keep the Chief Administrative Officer (CAO) and his staff fully aware of the extent of this problem and the costs involved in complying. This activity may require that the CAO recommend changing some aspects of the Zero-based budgeting methods currently used to allocate funds to the IT Department to pay for necessary personnel and software. This possible change in budgeting methods is something that should not be postponed beyond the current fiscal year.

F5. Everyone involved must realize that this area of the law is in a constant state of change, both at the state and federal level, and that there may even be some aspects of international Privacy laws that come into play at times, even for locally stored data.

F6. Of particular concern should be those Privacy laws relating to health records used or maintained by County agencies like Natividad Medical Center and the County Health Department since the provisions of the Federal HIPAA law are particularly burdensome and the penalties very expensive if violated.

F7. County departments and those agencies and personnel involved in acquisition of communications, software and almost every other type of goods and services, must insist both contractually and in practice that all vendors at every level comply with required Privacy and Breach Notice laws when dealing with County owned or controlled personal

data and information. Unfortunately, many commercial vendors and businesses are not currently in compliance, worldwide, as can be seen from the numerous data breaches recently reported in the U.S. news media.

F8. Finally, Monterey County is not unique in dealing with these critical Privacy problems, according to a story in the IAPP newsletter in late May 2014. This publication reported that the Los Angeles (LA) County Board of Supervisors recently voted to direct its county staff to promptly develop a plan to require third-party contractors hired by the County to "encrypt sensitive information on their computers as a condition of their contracts." This followed the February 2014 breach of data on eight computers holding 342,000 patients' medical records taken from the offices of contractor Sutherland Healthcare Solutions. LA County already mandates that county laptops be encrypted. These new rules now also require that all county department's computer workstations' hard drives are to be encrypted.

RECOMMENDATIONS

The CGJ makes the following Recommendations, based on the Facts and Conclusions discussed and reached in the foregoing investigative Report:

R1. The Monterey County Board of Supervisors and their staff should carefully study this Report on Privacy problems, in conjunction with its CAO, the County Counsel and his Privacy Deputy, and the Director of County Information Technology and her Security Chief and other IT personnel. These are key people since they directly work in the field of privacy, prevention of data breaches, and in coordinating the design and operation of the County website. The study of these issues has a dual purpose of understanding the significant penalties and financial risks to the County government due to the complexity of the laws, *and* realizing that there are some expensive and complex technical issues in this aspect of County business operations.

R2. The Board of Supervisors should consider the immediate need for additional funding to be provided both to County Counsel and the IT Department in order to improve existing and continuing compliance with California and Federal Privacy laws, rules and regulations. The CGJ believes funding at least one additional full time legal position for the County Counsel's office is imperative at this point, to help protect the County and its citizens. The IT Department also needs more funds to acquire and use various protective software packages that warn of impending attempts at data intrusion and stop them; and perhaps for one additional key person to head and direct the development and continuing maintenance of the County website on behalf of its many departments and agencies.

R3. County Counsel's office should promptly take all steps necessary to formally designate one of its lawyers as "County Privacy Law Counsel" and to provide for that person's continuing legal education in this extremely complex area of the law. This should include education to the point of certification of his or her knowledge in this field by the IAPP, the standard of this industry. We have been told portions of such proposed actions are currently underway.

R4. The duties of such Privacy Counsel should encompass working closely on a *continuous* basis with the IT Privacy Directors and County Department managers on *existing* and future Privacy Policies, and on all proposed contracts where vendors may have access to County records, and on all software licenses with third-party vendors. Privacy Counsel also needs to monitor closely these ever-changing laws to be certain that when changes in such laws occur these modified legal obligations and requirements are promptly communicated to responsible County personnel; so that they can be reflected quickly in then existing Policies; and so that follow-up educational meetings can be made for County personnel who must comply with these new laws.

R5. The County Information Technology Department Director and the Chief Security & Privacy Officer, working with the Security and Privacy Officers in other Departments, should be commended for the recent massive revision of Monterey County Privacy and Security Policies. This critical project has been on-going for more than for six years, in order to replace the existing, obsolete 2002-2004 versions. Unfortunately, these old Policies, as of May 2014, were still posted on the IT Department website, as well as a 2008 version which apparently still exists but is accessible only internally. In an effort to reduce County exposure for failure to comply with existing California and Federal Laws, and in fairness to Monterey County residents, prompt completion and dissemination of these revised Privacy and Security Policies should be a priority, especially since large amounts of Personally Identifiable Information ("PII") could otherwise be at risk of illegal disclosure.

R6. Finally, the CGJ strongly recommends that the subject of education about compliance by all County employees and their departments with California and Federal Privacy and Security laws be taken more seriously. We understand that existing County Policies call for such education efforts in the form of providing and requiring attendance at biennial educational programs. Several CGJ members actually attended the current educational program, which was well presented and current. However, employees from the highest to the lowest level of County government must be made to realize that, while these Policies, rules and laws may seem burdensome and inconvenient, failure to comply may not only result in loss of their jobs, but also in massive and punitive penalties and legal fees

incurred by the County if any such violations were to be litigated. This educational process is not an easy, nor inexpensive, task, but it must not be minimized.

RESPONSES REQUIRED

Pursuant to Penal Code Section 933.05, the CGJ requests Responses to all Findings and Recommendations by and from the Monterey County Board of Supervisors.

-END-