

**BRICCIO “RICKY” A. POLLO, PETITIONER, VS.
CHAIRPERSON KARINA CONSTANTINO-DAVID, DIRECTOR IV
RACQUEL DE GUZMAN BUENSALIDA, DIRECTOR IV LYDIA A.
CASTILLO, DIRECTOR III ENGELBERT A...**

G.R. No. 181881. October 18, 2011

Ponente: VILLARAMA, JR., J.

Read online (full-text search, related cases, audio case brief): <https://batas.org/library/g-r-no-181881/>

VILLARAMA, JR., J.:

This case involves a search of office computer assigned to a government employee who was charged administratively and eventually dismissed from the service. The employee's personal files stored in the computer were used by the government employer as evidence of misconduct.

Before us is a petition for review on certiorari under Rule 45 which seeks to reverse and set aside the Decision[1] dated October 11, 2007 and Resolution[2] dated February 29, 2008 of the Court of Appeals (CA). The CA dismissed the petition for certiorari (CA-G.R. SP No. 98224) filed by petitioner Briccio "Ricky" A. Pollo to nullify the proceedings conducted by the Civil Service Commission (CSC) which found him guilty of dishonesty, grave misconduct, conduct prejudicial to the best interest of the service, and violation of Republic Act (R.A.) No. 6713 and penalized him with dismissal.

The factual antecedents:

Petitioner is a former Supervising Personnel Specialist of the CSC Regional Office No. IV and also the Officer-in-Charge of the Public Assistance and Liaison Division (PALD) under the "Mamamayan Muna Hindi Mamaya Na" program of the CSC.

On January 3, 2007 at around 2:30 p.m., an unsigned letter-complaint addressed to respondent CSC Chairperson Karina Constantino-David which was marked "Confidential" and sent through a courier service (LBC) from a certain "Alan San Pascual" of Bagong Silang, Caloocan City, was received by the Integrated Records Management Office (IRMO) at the CSC Central Office. Following office practice in which documents marked "Confidential" are left unopened and instead sent to the addressee, the aforesaid letter was given directly to Chairperson David.

The letter-complaint reads:

The Chairwoman
Civil Service Commission
Batasan Hills, Quezon City

Dear Madam Chairwoman,

Belated Merry Christmas and Advance Happy New Year!

As a concerned citizen of my beloved country, I would like to ask from you personally if it is just alright for an

employee of your agency to be a lawyer of an accused gov't employee having a pending case in the csc. I honestly think this is a violation of law and unfair to others and your office.

I have known that a person have been lawyered by one of your attorney in the region 4 office. He is the chief of the Mamamayan muna hindi mamaya na division. He have been helping many who have pending cases in the Csc. The justice in our gov't system will not be served if this will continue. Please investigate this anomaly because our perception of your clean and good office is being tainted.

Concerned Govt employee[3]

Chairperson David immediately formed a team of four personnel with background in information technology (IT), and issued a memo directing them to conduct an investigation and specifically "to back up all the files in the computers found in the Mamamayan Muna (PALD) and Legal divisions." [4] After some briefing, the team proceeded at once to the CSC-ROIV office at Panay Avenue, Quezon City. Upon their arrival thereat around 5:30 p.m., the team informed the officials of the CSC-ROIV, respondents Director IV Lydia Castillo (Director Castillo) and Director III Engelbert Unite (Director Unite) of Chairperson David's directive.

The backing-up of all files in the hard disk of computers at the PALD and Legal Services Division (LSD) was witnessed by several employees, together with Directors Castillo and Unite who closely monitored said activity. At around 6:00 p.m., Director Unite sent text messages to petitioner and the head of LSD, who were both out of the office at the time, informing them of the ongoing copying of computer files in their divisions upon orders of the CSC Chair. The text messages received by petitioner read:

"Gud p.m. This is Atty. Unite FYI: Co people are going over the PCs of PALD and LSD per instruction of the Chairman. If you can make it here now it would be better."

"All PCs Of PALD and LSD are being backed up per memo of the chair."

"CO IT people arrived just now for this purpose. We were not also informed about this."

"We can't do anything about ... it ... it's a directive from chair."

"Memo of the chair was referring to an anonymous complaint"; "ill send a copy of the memo via mms" [5]

Petitioner replied also thru text message that he was leaving the matter to Director Unite and that he will just get a lawyer. Another text message received by petitioner from PALD staff also reported the presence of the team from CSC main office: "Sir may mga taga C.O. daw sa kuarto natin." [6] At around 10:00 p.m. of the same day, the investigating team finished their task. The next day, all the computers in the PALD were sealed and secured for the purpose of preserving all the files stored therein. Several diskettes containing the back-up files sourced from the hard disk of PALD and LSD computers were turned over to Chairperson David. The contents of the diskettes were examined by the CSC's Office for Legal Affairs (OLA). It was found that most of the files in the 17 diskettes containing files copied from the computer assigned to and being used by the petitioner, numbering about 40 to 42 documents, were draft pleadings or letters [7] in connection with administrative cases in the CSC and other tribunals. On the basis of this finding, Chairperson David issued the Show-Cause Order [8] dated January 11, 2007, requiring the petitioner, who had gone on extended leave, to submit his explanation or counter-affidavit within five days from notice.

Evaluating the subject documents obtained from petitioner's personal files, Chairperson David made the following observations:

Most of the foregoing files are drafts of legal pleadings or documents that are related to or connected with administrative cases that may broadly be lumped as pending either in the CSCRO No. IV, the CSC-NCR, the

CSC-Central Office or other tribunals. It is also of note that most of these draft pleadings are for and on behalves of parties, who are facing charges as respondents in administrative cases. This gives rise to the inference that the one who prepared them was knowingly, deliberately and willfully aiding and advancing interests adverse and inimical to the interest of the CSC as the central personnel agency of the government tasked to discipline misfeasance and malfeasance in the government service. The number of pleadings so prepared further demonstrates that such person is not merely engaged in an isolated practice but pursues it with seeming regularity. It would also be the height of naivete or credulity, and certainly against common human experience, to believe that the person concerned had engaged in this customary practice without any consideration, and in fact, one of the retrieved files (item 13 above) appears to insinuate the collection of fees. That these draft pleadings were obtained from the computer assigned to Pollo invariably raises the presumption that he was the one responsible or had a hand in their drafting or preparation since the computer of origin was within his direct control and disposition.[9]

Petitioner filed his Comment, denying that he is the person referred to in the anonymous letter-complaint which had no attachments to it, because he is not a lawyer and neither is he "lawyering" for people with cases in the CSC. He accused CSC officials of conducting a "fishing expedition" when they unlawfully copied and printed personal files in his computer, and subsequently asking him to submit his comment which violated his right against self-incrimination. He asserted that he had protested the unlawful taking of his computer done while he was on leave, citing the letter dated January 8, 2007 in which he informed Director Castillo that the files in his computer were his personal files and those of his sister, relatives, friends and some associates and that he is not authorizing their sealing, copying, duplicating and printing as these would violate his constitutional right to privacy and protection against self-incrimination and warrantless search and seizure. He pointed out that though government property, the temporary use and ownership of the computer issued under a Memorandum of Receipt (MR) is ceded to the employee who may exercise all attributes of ownership, including its use for personal purposes. As to the anonymous letter, petitioner argued that it is not actionable as it failed to comply with the requirements of a formal complaint under the Uniform Rules on Administrative Cases in the Civil Service (URACC). In view of the illegal search, the files/documents copied from his computer without his consent is thus inadmissible as evidence, being "fruits of a poisonous tree." [10]

On February 26, 2007, the CSC issued Resolution No. 070382[11] finding prima facie case against the petitioner and charging him with Dishonesty, Grave Misconduct, Conduct Prejudicial to the Best Interest of the Service and Violation of R.A. No. 6713 (Code of Conduct and Ethical Standards for Public Officials and Employees). Petitioner was directed to submit his answer under oath within five days from notice and indicate whether he elects a formal investigation. Since the charges fall under Section 19 of the URACC, petitioner was likewise placed under 90 days preventive suspension effective immediately upon receipt of the resolution. Petitioner received a copy of Resolution No. 070382 on March 1, 2007.

Petitioner filed an Omnibus Motion (For Reconsideration, to Dismiss and/or to Defer) assailing the formal charge as without basis having proceeded from an illegal search which is beyond the authority of the CSC Chairman, such power pertaining solely to the court. Petitioner reiterated that he never aided any people with pending cases at the CSC and alleged that those files found in his computer were prepared not by him but by certain persons whom he permitted, at one time or another, to make use of his computer out of close association or friendship. Attached to the motion were the affidavit of Atty. Ponciano R. Solosa who entrusted his own files to be kept at petitioner's CPU and Atty. Eric N. Estrellado, the latter being Atty. Solosa's client who attested that petitioner had nothing to do with the pleadings or bill for legal fees because in truth he owed legal fees to Atty. Solosa and not to petitioner. Petitioner contended that the case should be deferred in view of the prejudicial question raised in the criminal complaint he filed before the Ombudsman against Director Buensalida, whom petitioner believes had instigated this administrative case. He also prayed for the lifting of the preventive suspension imposed on him. In

its Resolution No. 070519[12] dated March 19, 2007, the CSC denied the omnibus motion. The CSC resolved to treat the said motion as petitioner's answer.

On March 14, 2007, petitioner filed an Urgent Petition[13] under Rule 65 of the Rules of Court, docketed as CA-G.R. SP No. 98224, assailing both the January 11, 2007 Show-Cause Order and Resolution No. 070382 dated February 26, 2007 as having been issued with grave abuse of discretion amounting to excess or total absence of jurisdiction. Prior to this, however, petitioner lodged an administrative/criminal complaint against respondents Directors Racquel D.G. Buensalida (Chief of Staff, Office of the CSC Chairman) and Lydia A. Castillo (CSC-RO IV) before the Office of the Ombudsman, and a separate complaint for disbarment against Director Buensalida.[14]

On April 17, 2007, petitioner received a notice of hearing from the CSC setting the formal investigation of the case on April 30, 2007. On April 25, 2007, he filed in the CA an Urgent Motion for the issuance of TRO and preliminary injunction.[15] Since he failed to attend the pre-hearing conference scheduled on April 30, 2007, the CSC reset the same to May 17, 2007 with warning that the failure of petitioner and/or his counsel to appear in the said pre-hearing conference shall entitle the prosecution to proceed with the formal investigation ex-parte.[16] Petitioner moved to defer or to reset the pre-hearing conference, claiming that the investigation proceedings should be held in abeyance pending the resolution of his petition by the CA. The CSC denied his request and again scheduled the pre-hearing conference on May 18, 2007 with similar warning on the consequences of petitioner and/or his counsel's non-appearance.[17] This prompted petitioner to file another motion in the CA, to cite the respondents, including the hearing officer, in indirect contempt.[18]

On June 12, 2007, the CSC issued Resolution No. 071134[19] denying petitioner's motion to set aside the denial of his motion to defer the proceedings and to inhibit the designated hearing officer, Atty. Bernard G. Jimenez. The hearing officer was directed to proceed with the investigation proper with dispatch.

In view of the absence of petitioner and his counsel, and upon the motion of the prosecution, petitioner was deemed to have waived his right to the formal investigation which then proceeded ex parte.

On July 24, 2007, the CSC issued Resolution No. 071420,[20] the dispositive part of which reads:

WHEREFORE, foregoing premises considered, the Commission hereby finds Briccio A. Pollo, a.k.a. Ricky A. Pollo GUILTY of Dishonesty, Grave Misconduct, Conduct Prejudicial to the Best Interest of the Service and Violation of Republic Act 6713. He is meted the penalty of DISMISSAL FROM THE SERVICE with all its accessory penalties, namely, disqualification to hold public office, forfeiture of retirement benefits, cancellation of civil service eligibilities and bar from taking future civil service examinations.[21]

On the paramount issue of the legality of the search conducted on petitioner's computer, the CSC noted the dearth of jurisprudence relevant to the factual milieu of this case where the government as employer invades the private files of an employee stored in the computer assigned to him for his official use, in the course of initial investigation of possible misconduct committed by said employee and without the latter's consent or participation. The CSC thus turned to relevant rulings of the United States Supreme Court, and cited the leading case of *O'Connor v. Ortega*[22] as authority for the view that government agencies, in their capacity as employers, rather than law enforcers, could validly conduct search and seizure in the governmental workplace without meeting the "probable cause" or warrant requirement for search and seizure. Another ruling cited by the CSC is the more recent case of *United States v. Mark L. Simons*[23] which declared that the federal agency's computer use policy foreclosed any inference of reasonable expectation of privacy on the part of its employees. Though the Court therein recognized that such policy did not, at the same time, erode the respondent's legitimate expectation of privacy in the office in which the computer was installed, still, the warrantless search of the employee's office was

upheld as valid because a government employer is entitled to conduct a warrantless search pursuant to an investigation of work-related misconduct provided the search is reasonable in its inception and scope.

With the foregoing American jurisprudence as benchmark, the CSC held that petitioner has no reasonable expectation of privacy with regard to the computer he was using in the regional office in view of the CSC computer use policy which unequivocally declared that a CSC employee cannot assert any privacy right to a computer assigned to him. Even assuming that there was no such administrative policy, the CSC was of the view that the search of petitioner's computer successfully passed the test of reasonableness for warrantless searches in the workplace as enunciated in the aforecited authorities. The CSC stressed that it pursued the search in its capacity as government employer and that it was undertaken in connection with an investigation involving work-related misconduct, which exempts it from the warrant requirement under the Constitution. With the matter of admissibility of the evidence having been resolved, the CSC then ruled that the totality of evidence adequately supports the charges of grave misconduct, dishonesty, conduct prejudicial to the best interest of the service and violation of R.A. No. 6713 against the petitioner. These grave infractions justified petitioner's dismissal from the service with all its accessory penalties.

In his Memorandum[24] filed in the CA, petitioner moved to incorporate the above resolution dismissing him from the service in his main petition, in lieu of the filing of an appeal via a Rule 43 petition. In a subsequent motion, he likewise prayed for the inclusion of Resolution No. 071800[25] which denied his motion for reconsideration.

By Decision dated October 11, 2007, the CA dismissed the petition for certiorari after finding no grave abuse of discretion committed by respondents CSC officials. The CA held that: (1) petitioner was not charged on the basis of the anonymous letter but from the initiative of the CSC after a fact-finding investigation was conducted and the results thereof yielded a prima facie case against him; (2) it could not be said that in ordering the back-up of files in petitioner's computer and later confiscating the same, Chairperson David had encroached on the authority of a judge in view of the CSC computer policy declaring the computers as government property and that employee-users thereof have no reasonable expectation of privacy in anything they create, store, send, or receive on the computer system; and (3) there is nothing contemptuous in CSC's act of proceeding with the formal investigation as there was no restraining order or injunction issued by the CA.

His motion for reconsideration having been denied by the CA, petitioner brought this appeal arguing that -

I

THE HONORABLE COURT OF APPEALS GRIEVOUSLY ERRED AND COMMITTED SERIOUS IRREGULARITY AND BLATANT ERRORS IN LAW AMOUNTING TO GRAVE ABUSE OF DISCRETION WHEN IT RULED THAT ANONYMOUS COMPLAINT IS ACTIONABLE UNDER E.O. 292 WHEN IN TRUTH AND IN FACT THE CONTRARY IS EXPLICITLY PROVIDED UNDER 2[nd] PARAGRAPH OF SECTION 8 OF CSC RESOLUTION NO. 99-1936, WHICH IS AN [AMENDMENT] TO THE ORIGINAL RULES PER CSC RESOLUTION NO. 94-0521;

II

THE HONORABLE COURT GRIEVOUSLY ERRED AND COMMITTED PALPABLE ERRORS IN LAW AMOUNTING TO GRAVE ABUSE OF DISCRETION WHEN IT RULED THAT PETITIONER CANNOT INVOKE HIS RIGHT TO PRIVACY, TO UNREASONABLE SEARCH AND SEIZURE, AGAINST SELF-INCRIMINATION, BY VIRTUE OF OFFICE MEMORANDUM NO. 10 S. 2002, A MERE INTERNAL MEMORANDUM SIGNED SOLELY AND EXCLUSIVELY BY RESPONDENT DAVID AND NOT BY THE COLLEGIAL COMMISSION CONSIDERING THAT POLICY MATTERS INVOLVING SUB[S]TANTIAL RIGHTS CANNOT BE COVERED BY AN OFFICE MEMORANDUM

WHICH IS LIMITED TO PROCEDURAL AND ROUTINARY INSTRUCTION;

III

THE HONORABLE COURT GRAVELY ERRED AND COMMITTED GRAVE ABUSE OF DISCRETION WHEN IT RULED THAT MEMO SEARCH DATED JANUARY 3, 2007 AND THE TAKING OF DOCUMENTS IN THE EVENING THEREOF FROM 7:00 TO 10:00 P.M. IS NOT GRAVE ABUSE OF DISCRETION LIMITING THE DEFINITION [OF] GRAVE ABUSE OF DISCRETION TO ONE INVOLVING AND TAINTED WITH PERSONAL HOSTILITY. IT LIKewise ERRED IN HOLDING THAT DATA STORED IN THE GOVERNMENT COMPUTERS ARE GOVERNMENT PROPERTIES INCLUDING THE PERSONAL FILES WHEN THE CONTRARY IS PROVIDED UNDER SECTION 14 OF OM. 10 s. 2002. AND GRIEVOUSLY ERRED STILL WHEN IT RULED THAT RESPONDENT DAVID BY VIRTUE OF O.M. 10 DID NOT ENCROACH ON THE DUTIES AND FUNCTIONS OF A JUDGE PURSUANT TO ARTICLE III, SECTION 2 OF THE 1987 PHILIPPINE CONSTITUTION;

IV

THE HONORABLE COURT ERRED WHEN IT FAILED TO CONSIDER ALL OTHER NEW ARGUMENTS, ADDITIONAL EVIDENCE HEREUNTO SUBMITTED AS WELL AS ITS FAILURE TO EVALUATE AND TAKE ACTION ON THE 2 MOTIONS TO ADMIT AND INCORPORATE CSC RESOLUTION NOS. 07-1420 DATED JULY 24, 2007 AND CSC RESOLUTION 07-1800 DATED SEPTEMBER 10, 2007. IT DID NOT RULE LIKewise ON THE FOUR URGENT MOTION TO RESOLVE ANCILLARY PRAYER FOR TRO.[26]

Squarely raised by the petitioner is the legality of the search conducted on his office computer and the copying of his personal files without his knowledge and consent, alleged as a transgression on his constitutional right to privacy.

The right to privacy has been accorded recognition in this jurisdiction as a facet of the right protected by the guarantee against unreasonable search and seizure under Section 2, Article III of the 1987 Constitution,[27] which provides:

Sec. 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

The constitutional guarantee is not a prohibition of all searches and seizures but only of "unreasonable" searches and seizures.[28] But to fully understand this concept and application for the purpose of resolving the issue at hand, it is essential that we examine the doctrine in the light of pronouncements in another jurisdiction. As the Court declared in *People v. Marti*[29]:

Our present constitutional provision on the guarantee against unreasonable search and seizure had its origin in the 1935 Charter which, worded as follows:

"The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no warrants shall issue but upon probable cause, to be determined by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched, and the persons or things to be seized." (Sec. 1[3], Article III)

was in turn derived almost verbatim from the Fourth Amendment to the United States Constitution. As such, the Court may turn to the pronouncements of the United States Federal Supreme Court and State Appellate Courts

which are considered doctrinal in this jurisdiction.[30]

In the 1967 case of *Katz v. United States*,[31] the US Supreme Court held that the act of FBI agents in electronically recording a conversation made by petitioner in an enclosed public telephone booth violated his right to privacy and constituted a "search and seizure". Because the petitioner had a reasonable expectation of privacy in using the enclosed booth to make a personal telephone call, the protection of the Fourth Amendment extends to such area. In the concurring opinion of Mr. Justice Harlan, it was further noted that the existence of privacy right under prior decisions involved a two-fold requirement: first, that a person has exhibited an actual (subjective) expectation of privacy; and second, that the expectation be one that society is prepared to recognize as reasonable (objective).[32]

In *Mancusi v. DeForte*[33] which addressed the reasonable expectations of private employees in the workplace, the US Supreme Court held that a union employee had Fourth Amendment rights with regard to an office at union headquarters that he shared with other union officials, even as the latter or their guests could enter the office. The Court thus "recognized that employees may have a reasonable expectation of privacy against intrusions by police."

That the Fourth Amendment equally applies to a government workplace was addressed in the 1987 case of *O'Connor v. Ortega*[34] where a physician, Dr. Magno Ortega, who was employed by a state hospital, claimed a violation of his Fourth Amendment rights when hospital officials investigating charges of mismanagement of the psychiatric residency program, sexual harassment of female hospital employees and other irregularities involving his private patients under the state medical aid program, searched his office and seized personal items from his desk and filing cabinets. In that case, the Court categorically declared that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." [35] A plurality of four Justices concurred that the correct analysis has two steps: first, because "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable", a court must consider "[t]he operational realities of the workplace" in order to determine whether an employee's Fourth Amendment rights are implicated; and next, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances." [36]

On the matter of government employees' reasonable expectations of privacy in their workplace, O'Connor teaches:

x x x Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation. x x x The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others - such as fellow employees, supervisors, consensual visitors, and the general public - may have frequent access to an individual's office. We agree with JUSTICE SCALIA that "[c]onstitutional protection against unreasonable searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer," x x x but some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. x x x Given the great variety of work environments in the public sector, the question of whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.[37] (Citations omitted; emphasis supplied.)

On the basis of the established rule in previous cases, the US Supreme Court declared that Dr. Ortega's Fourth Amendment rights are implicated only if the conduct of the hospital officials infringed "an expectation of privacy

that society is prepared to consider as reasonable." Given the undisputed evidence that respondent Dr. Ortega did not share his desk or file cabinets with any other employees, kept personal correspondence and other private items in his own office while those work-related files (on physicians in residency training) were stored outside his office, and there being no evidence that the hospital had established any reasonable regulation or policy discouraging employees from storing personal papers and effects in their desks or file cabinets (although the absence of such a policy does not create any expectation of privacy where it would not otherwise exist), the Court concluded that Dr. Ortega has a reasonable expectation of privacy at least in his desk and file cabinets.[38]

Proceeding to the next inquiry as to whether the search conducted by hospital officials was reasonable, the O'Connor plurality decision discussed the following principles:

Having determined that Dr. Ortega had a reasonable expectation of privacy in his office, the Court of Appeals simply concluded without discussion that the "search...was not a reasonable search under the fourth amendment." x x x "[t]o hold that the Fourth Amendment applies to searches conducted by [public employers] is only to begin the inquiry into the standards governing such searches...[W]hat is reasonable depends on the context within which a search takes place. x x x Thus, we must determine the appropriate standard of reasonableness applicable to the search. A determination of the standard of reasonableness applicable to a particular class of searches requires "balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." x x x In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.

x x x x

In our view, requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome. Imposing unwieldy warrant procedures in such cases upon supervisors, who would otherwise have no reason to be familiar with such procedures, is simply unreasonable. In contrast to other circumstances in which we have required warrants, supervisors in offices such as at the Hospital are hardly in the business of investigating the violation of criminal laws. Rather, work-related searches are merely incident to the primary business of the agency. Under these circumstances, the imposition of a warrant requirement would conflict with the "common-sense realization that government offices could not function if every employment decision became a constitutional matter." x x x

x x x x

The governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace. Government agencies provide myriad services to the public, and the work of these agencies would suffer if employers were required to have probable cause before they entered an employee's desk for the purpose of finding a file or piece of office correspondence. Indeed, it is difficult to give the concept of probable cause, rooted as it is in the criminal investigatory context, much meaning when the purpose of a search is to retrieve a file for work-related reasons. Similarly, the concept of probable cause has little meaning for a routine inventory conducted by public employers for the purpose of securing state property. x x x To ensure the efficient and proper operation of the agency, therefore, public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons.

We come to a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct. Even when employers conduct an investigation, they have an interest substantially different from "the normal need for law enforcement." x x x Public employers have an interest in ensuring that their agencies operate in an effective and efficient manner, and the work of these agencies inevitably suffers from the inefficiency, incompetence, mismanagement, or other work-related misfeasance of its employees. Indeed, in

many cases, public employees are entrusted with tremendous responsibility, and the consequences of their misconduct or incompetence to both the agency and the public interest can be severe. In contrast to law enforcement officials, therefore, public employers are not enforcers of the criminal law; instead, public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner. In our view, therefore, a probable cause requirement for searches of the type at issue here would impose intolerable burdens on public employers. The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest. x x x

x x x x

In sum, we conclude that the "special needs, beyond the normal need for law enforcement make the...probable-cause requirement impracticable," x x x for legitimate, work-related noninvestigatory intrusions as well as investigations of work-related misconduct. A standard of reasonableness will neither unduly burden the efforts of government employers to ensure the efficient and proper operation of the workplace, nor authorize arbitrary intrusions upon the privacy of public employees. We hold, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable:

"Determining the reasonableness of any search involves a twofold inquiry: first, one must consider 'whether the...action was justified at its inception,' x x x ; second, one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place,'" x x x

Ordinarily, a search of an employee's office by a supervisor will be "justified at its inception" when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file. x x x The search will be permissible in its scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of ...the nature of the [misconduct]." x x x[39] (Citations omitted; emphasis supplied.)

Since the District Court granted summary judgment without a hearing on the factual dispute as to the character of the search and neither was there any finding made as to the scope of the search that was undertaken, the case was remanded to said court for the determination of the justification for the search and seizure, and evaluation of the reasonableness of both the inception of the search and its scope.

In O'Connor the Court recognized that "special needs" authorize warrantless searches involving public employees for work-related reasons. The Court thus laid down a balancing test under which government interests are weighed against the employee's reasonable expectation of privacy. This reasonableness test implicates neither probable cause nor the warrant requirement, which are related to law enforcement.[40]

O'Connor was applied in subsequent cases raising issues on employees' privacy rights in the workplace. One of these cases involved a government employer's search of an office computer, *United States v. Mark L. Simons*[41] where the defendant Simons, an employee of a division of the Central Intelligence Agency (CIA), was convicted of receiving and possessing materials containing child pornography. Simons was provided with an office which he did not share with anyone, and a computer with Internet access. The agency had instituted a policy on computer use stating that employees were to use the Internet for official government business only and that accessing unlawful material was specifically prohibited. The policy also stated that users shall understand that the agency will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate. CIA agents

instructed its contractor for the management of the agency's computer network, upon initial discovery of prohibited internet activity originating from Simons' computer, to conduct a remote monitoring and examination of Simons' computer. After confirming that Simons had indeed downloaded pictures that were pornographic in nature, all the files on the hard drive of Simon's computer were copied from a remote work station. Days later, the contractor's representative finally entered Simon's office, removed the original hard drive on Simon's computer, replaced it with a copy, and gave the original to the agency security officer. Thereafter, the agency secured warrants and searched Simons' office in the evening when Simons was not around. The search team copied the contents of Simons' computer; computer diskettes found in Simons' desk drawer; computer files stored on the zip drive or on zip drive diskettes; videotapes; and various documents, including personal correspondence. At his trial, Simons moved to suppress these evidence, arguing that the searches of his office and computer violated his Fourth Amendment rights. After a hearing, the district court denied the motion and Simons was found guilty as charged.

Simons appealed his convictions. The US Supreme Court ruled that the searches of Simons' computer and office did not violate his Fourth Amendment rights and the first search warrant was valid. It held that the search remains valid under the O'Connor exception to the warrant requirement because evidence of the crime was discovered in the course of an otherwise proper administrative inspection. Simons' violation of the agency's Internet policy happened also to be a violation of criminal law; this does not mean that said employer lost the capacity and interests of an employer. The warrantless entry into Simons' office was reasonable under the Fourth Amendment standard announced in O'Connor because at the inception of the search, the employer had "reasonable grounds for suspecting" that the hard drive would yield evidence of misconduct, as the employer was already aware that Simons had misused his Internet access to download over a thousand pornographic images. The retrieval of the hard drive was reasonably related to the objective of the search, and the search was not excessively intrusive. Thus, while Simons had a reasonable expectation of privacy in his office, he did not have such legitimate expectation of privacy with regard to the files in his computer.

x x x To establish a violation of his rights under the Fourth Amendment, Simons must first prove that he had a legitimate expectation of privacy in the place searched or the item seized. x x x And, in order to prove a legitimate expectation of privacy, Simons must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable. x x x

x x x x

x x x We conclude that the remote searches of Simons' computer did not violate his Fourth Amendment rights because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet. Additionally, we conclude that Simons' Fourth Amendment rights were not violated by FBIS' retrieval of Simons' hard drive from his office.

Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy. The policy clearly stated that FBIS would "audit, inspect, and/or monitor" employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, "as deemed appropriate." x x x This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use. x x x Accordingly, FBIS' actions in remotely searching and seizing the computer files Simons downloaded from the Internet did not violate the Fourth Amendment.

x x x x

The burden is on Simons to prove that he had a legitimate expectation of privacy in his office. x x x Here, Simons has shown that he had an office that he did not share. As noted above, the operational realities of Simons' workplace may have diminished his legitimate privacy expectations. However, there is no evidence in the record of any workplace practices, procedures, or regulations that had such an effect. We therefore conclude that, on this record, Simons possessed a legitimate expectation of privacy in his office.

x x x x

In the final analysis, this case involves an employee's supervisor entering the employee's government office and retrieving a piece of government equipment in which the employee had absolutely no expectation of privacy - equipment that the employer knew contained evidence of crimes committed by the employee in the employee's office. This situation may be contrasted with one in which the criminal acts of a government employee were unrelated to his employment. Here, there was a conjunction of the conduct that violated the employer's policy and the conduct that violated the criminal law. We consider that FBIS' intrusion into Simons' office to retrieve the hard drive is one in which a reasonable employer might engage. x x x[42] (Citations omitted; emphasis supplied.)

This Court, in *Social Justice Society (SJS) v. Dangerous Drugs Board*[43] which involved the constitutionality of a provision in R.A. No. 9165 requiring mandatory drug testing of candidates for public office, students of secondary and tertiary schools, officers and employees of public and private offices, and persons charged before the prosecutor's office with certain offenses, have also recognized the fact that there may be such legitimate intrusion of privacy in the workplace.

The first factor to consider in the matter of reasonableness is the nature of the privacy interest upon which the drug testing, which effects a search within the meaning of Sec. 2, Art. III of the Constitution, intrudes. In this case, the office or workplace serves as the backdrop for the analysis of the privacy expectation of the employees and the reasonableness of drug testing requirement. The employees' privacy interest in an office is to a large extent circumscribed by the company's work policies, the collective bargaining agreement, if any, entered into by management and the bargaining unit, and the inherent right of the employer to maintain discipline and efficiency in the workplace. Their privacy expectation in a regulated office environment is, in fine, reduced; and a degree of impingement upon such privacy has been upheld. (Emphasis supplied.)

Applying the analysis and principles announced in *O'Connor and Simons* to the case at bar, we now address the following questions: (1) Did petitioner have a reasonable expectation of privacy in his office and computer files?; and (2) Was the search authorized by the CSC Chair, the copying of the contents of the hard drive on petitioner's computer reasonable in its inception and scope?

In this inquiry, the relevant surrounding circumstances to consider include "(1) the employee's relationship to the item seized; (2) whether the item was in the immediate control of the employee when it was seized; and (3) whether the employee took actions to maintain his privacy in the item." These factors are relevant to both the subjective and objective prongs of the reasonableness inquiry, and we consider the two questions together.[44] Thus, where the employee used a password on his computer, did not share his office with co-workers and kept the same locked, he had a legitimate expectation of privacy and any search of that space and items located therein must comply with the Fourth Amendment.[45]

We answer the first in the negative. Petitioner failed to prove that he had an actual (subjective) expectation of privacy either in his office or government-issued computer which contained his personal files. Petitioner did not allege that he had a separate enclosed office which he did not share with anyone, or that his office was always locked and not open to other employees or visitors. Neither did he allege that he used passwords or adopted any means to prevent other employees from accessing his computer files. On the contrary, he submits that being in the public assistance office of the CSC-ROIV, he normally would have visitors in his office like friends, associates

and even unknown people, whom he even allowed to use his computer which to him seemed a trivial request. He described his office as "full of people, his friends, unknown people" and that in the past 22 years he had been discharging his functions at the PALD, he is "personally assisting incoming clients, receiving documents, drafting cases on appeals, in charge of accomplishment report, Mamamayan Muna Program, Public Sector Unionism, Correction of name, accreditation of service, and hardly had anytime for himself alone, that in fact he stays in the office as a paying customer." [46] Under this scenario, it can hardly be deduced that petitioner had such expectation of privacy that society would recognize as reasonable.

Moreover, even assuming arguendo, in the absence of allegation or proof of the aforementioned factual circumstances, that petitioner had at least a subjective expectation of privacy in his computer as he claims, such is negated by the presence of policy regulating the use of office computers, as in *Simons*.

Office Memorandum No. 10, S. 2002 "Computer Use Policy (CUP)" explicitly provides:

POLICY

- The Computer Resources are the property of the Civil Service Commission and may be used only for legitimate business purposes.
- Users shall be permitted access to Computer Resources to assist them in the performance of their respective jobs.
- Use of the Computer Resources is a privilege that may be revoked at any given time.

x x x x

No Expectation of Privacy

- No expectation of privacy. Users except the Members of the Commission shall not have an expectation of privacy in anything they create, store, send, or receive on the computer system.

The Head of the Office for Recruitment, Examination and Placement shall select and assign Users to handle the confidential examination data and processes.

- Waiver of privacy rights. Users expressly waive any right to privacy in anything they create, store, send, or receive on the computer through the Internet or any other computer network. Users understand that the CSC may use human or automated means to monitor the use of its Computer Resources.
- Non-exclusivity of Computer Resources. A computer resource is not a personal property or for the exclusive use of a User to whom a memorandum of receipt (MR) has been issued. It can be shared or operated by other users. However, he is accountable therefor and must insure its care and maintenance.

x x x x

Passwords

- Responsibility for passwords. Users shall be responsible for safeguarding their passwords for access to the computer system. Individual passwords shall not be printed, stored online, or given to others. Users shall be responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.
- Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. The Civil Service Commission has global passwords that permit access to all materials stored on its networked computer system regardless of whether those materials have been encoded

with a particular User's password. Only members of the Commission shall authorize the application of the said global passwords.

x x x x[47] (Emphasis supplied.)

The CSC in this case had implemented a policy that put its employees on notice that they have no expectation of privacy in anything they create, store, send or receive on the office computers, and that the CSC may monitor the use of the computer resources using both automated or human means. This implies that on-the-spot inspections may be done to ensure that the computer resources were used only for such legitimate business purposes.

One of the factors stated in O'Connor which are relevant in determining whether an employee's expectation of privacy in the workplace is reasonable is the existence of a workplace privacy policy.[48] In one case, the US Court of Appeals Eighth Circuit held that a state university employee has not shown that he had a reasonable expectation of privacy in his computer files where the university's computer policy, the computer user is informed not to expect privacy if the university has a legitimate reason to conduct a search. The user is specifically told that computer files, including e-mail, can be searched when the university is responding to a discovery request in the course of litigation. Petitioner employee thus cannot claim a violation of Fourth Amendment rights when university officials conducted a warrantless search of his computer for work-related materials.[49]

As to the second point of inquiry on the reasonableness of the search conducted on petitioner's computer, we answer in the affirmative.

The search of petitioner's computer files was conducted in connection with investigation of work-related misconduct prompted by an anonymous letter-complaint addressed to Chairperson David regarding anomalies in the CSC-ROIV where the head of the Mamamayan Muna Hindi Mamaya Na division is supposedly "lawyering" for individuals with pending cases in the CSC. Chairperson David stated in her sworn affidavit:

- That prior to this, as early as 2006, the undersigned has received several text messages from unknown sources advertng to certain anomalies in Civil Service Commission Regional Office IV (CSCRO IV) such as, staff working in another government agency, "selling" cases and aiding parties with pending cases, all done during office hours and involved the use of government properties;
- That said text messages were not investigated for lack of any verifiable leads and details sufficient to warrant an investigation;
- That the anonymous letter provided the lead and details as it pinpointed the persons and divisions involved in the alleged irregularities happening in CSCRO IV;
- That in view of the seriousness of the allegations of irregularities happening in CSCRO IV and its effect on the integrity of the Commission, I decided to form a team of Central Office staff to back up the files in the computers of the Public Assistance and Liaison Division (PALD) and Legal Division;

x x x x[50]

A search by a government employer of an employee's office is justified at inception when there are reasonable grounds for suspecting that it will turn up evidence that the employee is guilty of work-related misconduct.[51] Thus, in the 2004 case decided by the US Court of Appeals Eighth Circuit, it was held that where a government agency's computer use policy prohibited electronic messages with pornographic content and in addition expressly provided that employees do not have any personal privacy rights regarding their use of the agency information systems and technology, the government employee had no legitimate expectation of privacy as to the use and contents of his office computer, and therefore evidence found during warrantless search of the computer was admissible in prosecution for child pornography. In that case, the defendant employee's computer hard drive was

first remotely examined by a computer information technician after his supervisor received complaints that he was inaccessible and had copied and distributed non-work-related e-mail messages throughout the office. When the supervisor confirmed that defendant had used his computer to access the prohibited websites, in contravention of the express policy of the agency, his computer tower and floppy disks were taken and examined. A formal administrative investigation ensued and later search warrants were secured by the police department. The initial remote search of the hard drive of petitioner's computer, as well as the subsequent warrantless searches was held as valid under the O'Connor ruling that a public employer can investigate work-related misconduct so long as any search is justified at inception and is reasonably related in scope to the circumstances that justified it in the first place.[52]

Under the facts obtaining, the search conducted on petitioner's computer was justified at its inception and scope. We quote with approval the CSC's discussion on the reasonableness of its actions, consistent as it were with the guidelines established by O'Connor:

Even conceding for a moment that there is no such administrative policy, there is no doubt in the mind of the Commission that the search of Pollo's computer has successfully passed the test of reasonableness for warrantless searches in the workplace as enunciated in the above-discussed American authorities. It bears emphasis that the Commission pursued the search in its capacity as a government employer and that it was undertaken in connection with an investigation involving a work-related misconduct, one of the circumstances exempted from the warrant requirement. At the inception of the search, a complaint was received recounting that a certain division chief in the CSCRO No. IV was "lawyering" for parties having pending cases with the said regional office or in the Commission. The nature of the imputation was serious, as it was grievously disturbing. If, indeed, a CSC employee was found to be furtively engaged in the practice of "lawyering" for parties with pending cases before the Commission would be a highly repugnant scenario, then such a case would have shattering repercussions. It would undeniably cast clouds of doubt upon the institutional integrity of the Commission as a quasi-judicial agency, and in the process, render it less effective in fulfilling its mandate as an impartial and objective dispenser of administrative justice. It is settled that a court or an administrative tribunal must not only be actually impartial but must be seen to be so, otherwise the general public would not have any trust and confidence in it.

Considering the damaging nature of the accusation, the Commission had to act fast, if only to arrest or limit any possible adverse consequence or fall-out. Thus, on the same date that the complaint was received, a search was forthwith conducted involving the computer resources in the concerned regional office. That it was the computers that were subjected to the search was justified since these furnished the easiest means for an employee to encode and store documents. Indeed, the computers would be a likely starting point in ferreting out incriminating evidence. Concomitantly, the ephemeral nature of computer files, that is, they could easily be destroyed at a click of a button, necessitated drastic and immediate action. Pointedly, to impose the need to comply with the probable cause requirement would invariably defeat the purpose of the work-related investigation.

Worthy to mention, too, is the fact that the Commission effected the warrantless search in an open and transparent manner. Officials and some employees of the regional office, who happened to be in the vicinity, were on hand to observe the process until its completion. In addition, the respondent himself was duly notified, through text messaging, of the search and the concomitant retrieval of files from his computer.

All in all, the Commission is convinced that the warrantless search done on computer assigned to Pollo was not, in any way, vitiated with unconstitutionality. It was a reasonable exercise of the managerial prerogative of the Commission as an employer aimed at ensuring its operational effectiveness and efficiency by going after the work-related misfeasance of its employees. Consequently, the evidence derived from the questioned search are deemed admissible.[53]

Petitioner's claim of violation of his constitutional right to privacy must necessarily fail. His other argument invoking the privacy of communication and correspondence under Section 3(1), Article III of the 1987 Constitution is also untenable considering the recognition accorded to certain legitimate intrusions into the privacy of employees in the government workplace under the aforementioned authorities. We likewise find no merit in his contention that O'Connor and Simons are not relevant because the present case does not involve a criminal offense like child pornography. As already mentioned, the search of petitioner's computer was justified there being reasonable ground for suspecting that the files stored therein would yield incriminating evidence relevant to the investigation being conducted by CSC as government employer of such misconduct subject of the anonymous complaint. This situation clearly falls under the exception to the warrantless requirement in administrative searches defined in O'Connor.

The Court is not unaware of our decision in Anonymous Letter-Complaint against Atty. Miguel Morales, Clerk of Court, Metropolitan Trial Court of Manila[54] involving a branch clerk (Atty. Morales) who was investigated on the basis of an anonymous letter alleging that he was consuming his working hours filing and attending to personal cases, using office supplies, equipment and utilities. The OCA conducted a spot investigation aided by NBI agents. The team was able to access Atty. Morales' personal computer and print two documents stored in its hard drive, which turned out to be two pleadings, one filed in the CA and another in the RTC of Manila, both in the name of another lawyer. Atty. Morales' computer was seized and taken in custody of the OCA but was later ordered released on his motion, but with order to the MISO to first retrieve the files stored therein. The OCA disagreed with the report of the Investigating Judge that there was no evidence to support the charge against Atty. Morales as no one from the OCC personnel who were interviewed would give a categorical and positive statement affirming the charges against Atty. Morales, along with other court personnel also charged in the same case. The OCA recommended that Atty. Morales should be found guilty of gross misconduct. The Court En Banc held that while Atty. Morales may have fallen short of the exacting standards required of every court employee, the Court cannot use the evidence obtained from his personal computer against him for it violated his constitutional right against unreasonable searches and seizures. The Court found no evidence to support the claim of OCA that they were able to obtain the subject pleadings with the consent of Atty. Morales, as in fact the latter immediately filed an administrative case against the persons who conducted the spot investigation, questioning the validity of the investigation and specifically invoking his constitutional right against unreasonable search and seizure. And as there is no other evidence, apart from the pleadings, retrieved from the unduly confiscated personal computer of Atty. Morales, to hold him administratively liable, the Court had no choice but to dismiss the charges against him for insufficiency of evidence.

The above case is to be distinguished from the case at bar because, unlike the former which involved a personal computer of a court employee, the computer from which the personal files of herein petitioner were retrieved is a government-issued computer, hence government property the use of which the CSC has absolute right to regulate and monitor. Such relationship of the petitioner with the item seized (office computer) and other relevant factors and circumstances under American Fourth Amendment jurisprudence, notably the existence of CSC MO 10, S. 2007 on Computer Use Policy, failed to establish that petitioner had a reasonable expectation of privacy in the office computer assigned to him.

Having determined that the personal files copied from the office computer of petitioner are admissible in the administrative case against him, we now proceed to the issue of whether the CSC was correct in finding the petitioner guilty of the charges and dismissing him from the service.

Well-settled is the rule that the findings of fact of quasi-judicial agencies, like the CSC, are accorded not only respect but even finality if such findings are supported by substantial evidence. Substantial evidence is such

amount of relevant evidence which a reasonable mind might accept as adequate to support a conclusion, even if other equally reasonable minds might conceivably opine otherwise.[55]

The CSC based its findings on evidence consisting of a substantial number of drafts of legal pleadings and documents stored in his office computer, as well as the sworn affidavits and testimonies of the witnesses it presented during the formal investigation. According to the CSC, these documents were confirmed to be similar or exactly the same content-wise with those on the case records of some cases pending either with CSCRO No. IV, CSC-NCR or the Commission Proper. There were also substantially similar copies of those pleadings filed with the CA and duly furnished the Commission. Further, the CSC found the explanation given by petitioner, to the effect that those files retrieved from his computer hard drive actually belonged to his lawyer friends Estrellado and Solosa whom he allowed the use of his computer for drafting their pleadings in the cases they handle, as implausible and doubtful under the circumstances. We hold that the CSC's factual finding regarding the authorship of the subject pleadings and misuse of the office computer is well-supported by the evidence on record, thus:

It is also striking to note that some of these documents were in the nature of pleadings responding to the orders, decisions or resolutions of these offices or directly in opposition to them such as a petition for certiorari or a motion for reconsideration of CSC Resolution. This indicates that the author thereof knowingly and willingly participated in the promotion or advancement of the interests of parties contrary or antagonistic to the Commission. Worse, the appearance in one of the retrieved documents the phrase, "Eric N. Estr[e]llado, Epal kulang ang bayad mo," lends plausibility to an inference that the preparation or drafting of the legal pleadings was pursued with less than a laudable motivation. Whoever was responsible for these documents was simply doing the same for the money - a "legal mercenary" selling or purveying his expertise to the highest bidder, so to speak.

Inevitably, the fact that these documents were retrieved from the computer of Pollo raises the presumption that he was the author thereof. This is because he had a control of the said computer. More significantly, one of the witnesses, Margarita Reyes, categorically testified seeing a written copy of one of the pleadings found in the case records lying on the table of the respondent. This was the Petition for Review in the case of Estrellado addressed to the Court of Appeals. The said circumstances indubitably demonstrate that Pollo was secretly undermining the interest of the Commission, his very own employer.

To deflect any culpability, Pollo would, however, want the Commission to believe that the documents were the personal files of some of his friends, including one Attorney Ponciano Solosa, who incidentally served as his counsel of record during the formal investigation of this case. In fact, Atty. Solosa himself executed a sworn affidavit to this effect. Unfortunately, this contention of the respondent was directly rebutted by the prosecution witness, Reyes, who testified that during her entire stay in the PALD, she never saw Atty. Solosa using the computer assigned to the respondent. Reyes more particularly stated that she worked in close proximity with Pollo and would have known if Atty. Solosa, whom she personally knows, was using the computer in question. Further, Atty. Solosa himself was never presented during the formal investigation to confirm his sworn statement such that the same constitutes self-serving evidence unworthy of weight and credence. The same is true with the other supporting affidavits, which Pollo submitted.

At any rate, even admitting for a moment the said contention of the respondent, it evinces the fact that he was unlawfully authorizing private persons to use the computer assigned to him for official purpose, not only once but several times gauging by the number of pleadings, for ends not in conformity with the interests of the Commission. He was, in effect, acting as a principal by indispensable cooperation...Or at the very least, he should be responsible for serious misconduct for repeatedly allowing CSC resources, that is, the computer and the electricity, to be utilized for purposes other than what they were officially intended.

Further, the Commission cannot lend credence to the posturing of the appellant that the line appearing in one

of the documents, "Eric N. Estrellado, Epal kulang ang bayad mo," was a private joke between the person alluded to therein, Eric N. Estrellado, and his counsel, Atty. Solosa, and not indicative of anything more sinister. The same is too preposterous to be believed. Why would such a statement appear in a legal pleading stored in the computer assigned to the respondent, unless he had something to do with it?[56]

Petitioner assails the CA in not ruling that the CSC should not have entertained an anonymous complaint since Section 8 of CSC Resolution No. 99-1936 (URACC) requires a verified complaint:

Rule II - Disciplinary Cases

SEC. 8. Complaint. - A complaint against a civil service official or employee shall not be given due course unless it is in writing and subscribed and sworn to by the complainant. However, in cases initiated by the proper disciplining authority, the complaint need not be under oath.

No anonymous complaint shall be entertained unless there is obvious truth or merit to the allegation therein or supported by documentary or direct evidence, in which case the person complained of may be required to comment.

x x x x

We need not belabor this point raised by petitioner. The administrative complaint is deemed to have been initiated by the CSC itself when Chairperson David, after a spot inspection and search of the files stored in the hard drive of computers in the two divisions adverted to in the anonymous letter -- as part of the disciplining authority's own fact-finding investigation and information-gathering -- found a *prima facie* case against the petitioner who was then directed to file his comment. As this Court held in *Civil Service Commission v. Court of Appeals*[57] --

Under Sections 46 and 48 (1), Chapter 6, Subtitle A, Book V of E.O. No. 292 and Section 8, Rule II of Uniform Rules on Administrative Cases in the Civil Service, a complaint may be initiated against a civil service officer or employee by the appropriate disciplining authority, even without being subscribed and sworn to. Considering that the CSC, as the disciplining authority for Dumlao, filed the complaint, jurisdiction over Dumlao was validly acquired. (Emphasis supplied.)

As to petitioner's challenge on the validity of CSC OM 10, S. 2002 (CUP), the same deserves scant consideration. The alleged infirmity due to the said memorandum order having been issued solely by the CSC Chair and not the Commission as a collegial body, upon which the dissent of Commissioner Buenaflor is partly anchored, was already explained by Chairperson David in her Reply to the Addendum to Commissioner Buenaflor's previous memo expressing his dissent to the actions and disposition of the Commission in this case. According to Chairperson David, said memorandum order was in fact exhaustively discussed, provision by provision in the January 23, 2002 Commission Meeting, attended by her and former Commissioners Erestain, Jr. and Valmores. Hence, the Commission En Banc at the time saw no need to issue a Resolution for the purpose and further because the CUP being for internal use of the Commission, the practice had been to issue a memorandum order.[58] Moreover, being an administrative rule that is merely internal in nature, or which regulates only the personnel of the CSC and not the public, the CUP need not be published prior to its effectivity.[59]

In fine, no error or grave abuse of discretion was committed by the CA in affirming the CSC's ruling that petitioner is guilty of grave misconduct, dishonesty, conduct prejudicial to the best interest of the service, and violation of R.A. No. 6713. The gravity of these offenses justified the imposition on petitioner of the ultimate penalty of dismissal with all its accessory penalties, pursuant to existing rules and regulations.

WHEREFORE, the petition for review on certiorari is DENIED. The Decision dated October 11, 2007 and Resolution dated February 29, 2008 of the Court of Appeals in CA-G.R. SP No. 98224 are AFFIRMED.

With costs against the petitioner.

SO ORDERED.

Corona, C.J., Brion, Peralta, Perez, Mendoza, Reyes, and Perlas-Bernabe, JJ., concur.

Carpio, J., see separate opinion.

Velasco, Jr., J., joins opinion of J. Bersamin.

Leonardo-De Castro and Abad, JJ., joins the concurring and dissenting opinion of J. Bersamin.

Bersamin, J., please see concurring opinion and dissenting opinion.

Del Castillo, J., No part.

Sereno, J., concur but share J. Carpio's concerns.

[1] Rollo, pp. 63-83. Penned by Associate Justice Romeo F. Barza, with Associate Justices Mariano C. Del Castillo (now a Member of this Court) and Arcangelita M. Romilla-Lontok concurring.

[2] Id. at 85.

[3] Id. at 306.

[4] Id. at 305.

[5] CA rollo, p. 56.

[6] Id.

[7] Id. at 21-24.

[8] Id. at 20-25.

[9] Id. at 25.

[10] Id. at 55-62.

[11] Id. at 26-33. Chairperson Karina Constantino-David and Commissioner Mary Ann Z. Fernandez-Mendoza concurred in ruling that a prima facie case existed against petitioner while Commissioner Cesar D. Buenaflor dissented [see Memorandum (OCOM-C Memo No. 14, s. 2007, CA rollo, pp. 431-434).

[12] CSC records, pp. 71-l to 71-n. Chairperson Karina Constantino-David and Commissioner Mary Ann Z. Fernandez-Mendoza concurred in the denial of the omnibus motion while Commissioner Cesar D. Buenaflor reiterated his dissent.

[13] CA rollo, pp. 2-19.

[14] Id. at 288-294, 321-325.

[15] Id. at 336-340.

[16] Id. at 373.

[17] Id. at 376-378.

[18] Id. at 388-392.

[19] Id. at 457-463. Chairperson Karina Constantino-David and Commissioner Mary Ann Z. Fernandez-Mendoza concurred in denying the motion while Commissioner Cesar D. Buenaflor dissented stating that based on his

dissenting position, any subsequent proceedings in this case is of no moment since the initiatory proceedings was in violation of a person's fundamental rights enshrined in the Bill of Rights of the Constitution. (Id. at 465.)

[20] Id. at 586-618. Chairperson Karina Constantino-David and Commissioner Mary Ann Z. Fernandez-Mendoza concurred in ruling that petitioner is guilty as charged while Commissioner Cesar D. Buenaflor maintained his dissent.

[21] Id. at 618.

[22] 480 U.S. 709 (1987).

[23] 206 F.3d 392 (4th Cir. 2000).

[24] Id. at 560-585.

[25] Id. at 707-719. Chairperson Karina Constantino-David and Commissioner Mary Ann Z. Fernandez-Mendoza concurred in the denial of the motion for reconsideration while Commissioner Cesar D. Buenaflor reiterated his dissent under his "Addendum to the Dissenting Position Under OCOM-C Memo No. 14, S. 2007". (Id. at 720.)

[26] Rollo, p. 19.

[27] Social Justice Society (SJS) v. Dangerous Drugs Board, G.R. Nos. 157870, 158633 and 161658, November 3, 2008, 570 SCRA 410, 427, citing *Ople v. Torres*, G.R. No. 127685, July 23, 1998, 293 SCRA 141, 169.

[28] Joaquin Bernas, S.J., *The Constitution of the Republic of the Philippines: A Commentary*, 2003 ed., p. 162.

[29] G.R. No. 81561, January 18, 1991, 193 SCRA 57.

[30] Id. at 63.

[31] 389 U.S. 437 (1967).

[32] Id.

[33] 392 U.S. 364, 88 S.Ct. 2120, 20 L.Ed2d 1154 (1968).

[34] *Supra* note 22.

[35] Id. at 717.

[36] *City of Ontario, Cal. v. Quon*, 130 S.Ct. 2619, U.S. 2010, June 17, 2010.

[37] *Supra* note 22 at 717-718.

[38] Id. at 718-719.

[39] Id. at 719, 722-725.

[40] *Francis v. Giacomelli*, 588 F.3d 186, C.A. (Md), December 2, 2009.

[41] *Supra* note 23.

[42] Id.

[43] *Supra* note 27 at 432-433.

[44] *U.S. v. Barrows*, 481 F.3d 1246, C.A.10 (Okla.), April 3, 2007, citing *United States v. Anderson*, 154 F.3d

1225, 1229 (10[th] Cir. 1998).

[45] U.S. v. Ziegler, 474 F.3d 1184 C.A.9 (Mont.), January 30, 2007.

[46] CA rollo, pp. 42, 61.

[47] Id. at 440-443.

[48] Biby v. Board of Regents, of the University of Nebraska at Lincoln, 419 F.3d 845 C.A.8 (Neb), August 22, 2005.

[49] Id.

[50] CA rollo, p. 639.

[51] U.S. v. Thorn, 375 F.3d 679, C.A.8 (Mo.), July 13, 2004.

[52] Id.

[53] CA rollo, pp. 611-612.

[54] A.M. Nos. P-08-2519 and P-08-2520, November 19, 2008, 571 SCRA 361.

[55] Vertudes v. Buenaflor, G.R. No. 153166, December 16, 2005, 478 SCRA 210, 230, citing Rosario v. Victory Ricemill, G.R. No. 147572, February 19, 2003, 397 SCRA 760, 766 and Bagong Bayan Corp., Realty Investors and Developers v. NLRC, G.R. No. 61272, September 29, 1989, 178 SCRA 107.

[56] CA rollo, pp. 616-617.

[57] G.R. No. 147009, March 11, 2004, 425 SCRA 394, 401.

[58] Rollo, p. 299.

[59] See Tañada v. Hon. Tuvera, 230 Phil. 528, 535 (1986).

CONCURRING AND DISSENTING OPINION

BERSAMIN, J.:

I render this concurring and dissenting opinion only to express my thoughts on the constitutional right to privacy of communication and correspondence vis-à-vis an office memorandum that apparently removed an employee's expectation of privacy in the workplace.

I

Indispensable to the position I take herein is an appreciation of the development and different attributes of the right to privacy that has come to be generally regarded today as among the valuable rights of the individual that must be given Constitutional protection.

The 1890 publication in the Harvard Law Review of The Right to Privacy,[1] an article of 28 pages co-written by former law classmates Samuel Warren and Louis Brandeis, is often cited to have given birth to the recognition of the constitutional right to privacy. The article was spawned by the emerging growth of media and technology, with the co-authors particularly being concerned by the production in 1884 by the Eastman Kodak Company of a "snap camera" that enabled people to take candid pictures. Prior to 1884, cameras had been expensive and heavy;

they had to be set up and people would have to pose to have their pictures taken. The snap camera expectedly ignited the enthusiasm for amateur photography in thousands of people who had previously not been able to afford a camera. This technological development moved Warren and Brandeis to search for a legal right to protect individual privacy.[2] One of the significant assertions they made in their article was the declaration that "the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others,"[3] said right being merely part of an individual's right to be let alone.[4]

While some quarters do not easily concede that Warren and Brandeis "invented" the right to privacy, mainly because a robust body of confidentiality law protecting private information from disclosure existed throughout Anglo-American common law by 1890, critics have acknowledged that The Right to Privacy charted a new path for American privacy law.[5]

In 1928, Brandeis, already a Supreme Court Justice, incorporated the right to be let alone in his dissent in *Olmstead v. United States*,[6] viz:

"The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone ? the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth." [emphasis supplied]

In 1960, torts scholar William Prosser published in the *California Law Review*[7] his article *Privacy* based on his thorough review of the various decisions of the United States courts and of the privacy laws. He observed then that the "law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone.'"[8] He identified the four torts as: (a) the intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (b) the public disclosure of embarrassing private facts about the plaintiff; (c) the publicity that places the plaintiff in a false light in the public eye; and (d) the appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[9]

With regard to the first tort of intrusion upon seclusion or solitude, or into private affairs, Prosser posited that there was a remedy when a person "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns" in a manner that was "highly offensive to a reasonable person." [10] The second and third torts established liability when the publicized matter was highly offensive to a reasonable person and was not a legitimate concern of the public - if it involved disclosure of embarrassing private facts - or placed another before the public in a false light.[11] Lastly, the tort of appropriation afforded a relief when a person adopted "to his own use or benefit the name or likeness of another." [12]

In the 1977 landmark ruling of *Whalen v. Roe*, [13] the US Supreme Court expanded the right to privacy by categorizing privacy claims into two, namely: informational privacy, to refer to the interest in avoiding disclosure of personal matters; and decisional privacy, to refer to the interest in independence in making certain kinds of important decisions.

All US Circuit Courts recognizing informational privacy have held that this right is not absolute and, therefore, they have balanced individuals' informational privacy interests against the State's interest in acquiring or disclosing the information.[14] The majority of the US Circuit Courts have adopted some form of scrutiny that has required the Government to show a "substantial" interest for invading individuals' right to confidentiality in their personal information, and then to balance the State's substantial interest in the disclosure as against the individual's interest in confidentiality.[15] This balancing test was developed in *United States v. Westinghouse*[16] by using the following factors, to wit: (a) the type of record requested; (b) the information it did or might contain; (c) the potential for harm in any subsequent nonconsensual disclosure; (d) the injury from disclosure to the relationship in which the record was generated; (e) the adequacy of safeguards to prevent unauthorized disclosure; (f) the degree of need for access; and (g) the presence of an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[17]

Decisional privacy, on the other hand, evolved from decisions touching on matters concerning speech, religion, personal relations, education and sexual preferences. As early as 1923, the US Supreme Court recognized decisional privacy in its majority opinion in *Meyer v. Nebraska*.^[18] The petitioner therein was tried and convicted by a district court, and his conviction was affirmed by the Supreme Court of the Nebraska, for teaching the subject of reading in the German language to a ten-year old boy who had not attained and successfully passed eighth grade.^[19] In reversing the judgment, Justice McReynolds of the US Supreme Court pronounced that the liberty guaranteed by the Fourteenth Amendment "denotes not merely freedom from bodily restraint, but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men." Justice McReynolds elaborated thusly:

"Practically, education of the young is only possible in schools conducted by especially qualified persons who devote themselves thereto. The calling always has been regarded as useful and honorable, essential, indeed, to the public welfare. Mere knowledge of the German language cannot reasonably be regarded as harmful. Heretofore it has been commonly looked upon as helpful and desirable. Plaintiff in error taught this language in school as part of his occupation. His right thus to teach and the right of parents to engage him so to instruct their children, we think, are within the liberty of the Amendment."

In *Griswold v. Connecticut*,^[20] the US Supreme Court resolved another decisional privacy claim by striking down a statute that prohibited the use of contraceptives by married couples. Justice Douglas, delivering the opinion, declared:

"By *Pierce v. Society of Sisters*, supra, the right to educate one's children as one chooses is made applicable to the States by the force of the First and Fourteenth Amendments. By *Meyer v. Nebraska*, supra, the same dignity is given the right to study the German language in a private school. In other words, the State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge. The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read (*Martin v. Struthers*, 319 U.S. 141, 143) and freedom of inquiry, freedom of thought, and freedom to teach (see *Wiemann v. Updegraff*, 344 U.S. 183, 195) -- indeed, the freedom of the entire university community. (*Sweezy v. New Hampshire*, 354 U.S. 234, 249-250, 261-263; *Barenblatt v. United States*, 360 U.S. 109, 112; *Baggett v. Bullitt*, 377 U.S. 360, 369). Without those peripheral rights, the specific rights would be less secure. And so we reaffirm the principle of the *Pierce* and the *Meyer* cases.

x x x x

"The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. And it concerns a law which, in forbidding the use of contraceptives,

rather than regulating their manufacture or sale, seeks to achieve its goals by means having a maximum destructive impact upon that relationship. Such a law cannot stand in light of the familiar principle, so often applied by this Court, that a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms. (NAACP v. Alabama, 377 U.S. 288, 307). Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship."

One of the most controversial decisional privacy claims was dealt with in *Roe v. Wade*,^[21] by which the US Supreme Court justified abortion in the United States on the premise that:

"This right of privacy xxx is broad enough to encompass a woman's decision whether or not to terminate her pregnancy. The detriment that the State would impose upon the pregnant woman by denying this choice altogether is apparent. Specific and direct harm medically diagnosable even in early pregnancy may be involved. Maternity, or additional offspring, may force upon the woman a distressful life and future. Psychological harm may be imminent. Mental and physical health may be taxed by child care. There is also the distress, for all concerned, associated with the unwanted child, and there is the problem of bringing a child into a family already unable, psychologically and otherwise, to care for it. In other cases, as in this one, the additional difficulties and continuing stigma of unwed motherhood may be involved. All these are factors the woman and her responsible physician necessarily will consider in consultation.

x x x x

"Although the results are divided, most of these courts have agreed that the right of privacy, however based, is broad enough to cover the abortion decision; that the right, nonetheless, is not absolute and is subject to some limitations; and that at some point the state interests as to protection of health, medical standards, and prenatal life, become dominant."

In the Philippines, we have upheld decisional privacy claims. For instance, in the 2003 case of *Estrada v. Escritor*,^[22] although the majority opinion dealt extensively with the claim of religious freedom, a right explicitly provided by the Constitution, Justice Bellosillo's separate opinion was informative with regard to the privacy aspect of the issue involved and, hence, stated:

"More than religious freedom, I look with partiality to the rights of due process and privacy. Law in general reflects a particular morality or ideology, and so I would rather not foist upon the populace such criteria as "compelling state interest," but more, the reasonably foreseeable specific connection between an employee's potentially embarrassing conduct and the efficiency of the service. This is a fairly objective standard than the compelling interest standard involved in religious freedom.

"Verily, if we are to remand the instant case to the Office of the Court Administrator, we must also configure the rights of due process and privacy into the equation. By doing so, we can make a difference not only for those who object out of religious scruples but also for those who choose to live a meaningful life even if it means sometimes breaking "oppressive" and "antiquated" application of laws but are otherwise efficient and effective workers. As is often said, when we have learned to reverence each individual's liberty as we do our tangible wealth, we then shall have our renaissance."

Relevantly, Article III, Section 3 of the 1987 Constitution embodies the protection of the privacy of communication and correspondence, to wit:

Section 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

x x x x

Yet, the guarantee in favor of the privacy of communication and correspondence is not absolute, for it expressly allows intrusion either upon lawful order of a court or when public safety and order so demands (even without a court order).[23]

In its 1965 ruling in *Griswold v. Connecticut*,^[24] the US Supreme Court declared that the right to privacy was a fundamental personal right; and that the enumeration in the Constitution of certain rights should not be construed as a denial or disparagement of others that have been retained by the people,^[25] considering that the "specific guarantees in the Bill of Rights had penumbras, formed by emanations from those guarantees that helped give them life and substance." Accordingly, an individual's right to privacy of communication and correspondence cannot, as a general rule, be denied without violating the basic principles of liberty and justice.

The constitutional right to privacy in its Philippine context was first recognized in the 1968 ruling of *Morfe v. Mutuc*,^[26] where the Court affirmed that:

"The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection. The language of Prof. Emerson is particularly apt: "The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state. In contrast, a system of limited government, safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector -- protection, in other words, of the dignity and integrity of the individual -- has become increasingly important as modern society has developed. All the forces of a technological age -- industrialization, urbanization, and organization -- operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society."

Morfe v. Mutuc emphasized the significance of privacy by declaring that "[t]he right to be let alone is indeed the beginning of all freedom."^[27] The description hewed very closely to that earlier made by Justice Brandeis in *Olmstead v. United States* that the right to be let alone was "the most comprehensive of rights and the right most valued by civilized men."^[28]

It is elementary that before this constitutional right may be invoked a reasonable or objective expectation of privacy should exist, a concept that was introduced in the concurring opinion of Justice Harlan in the 1967 case *Katz v. United States*,^[29] no doubt inspired by the oral argument^[30] of Judge Harvey Schneider, then co-counsel for petitioner Charles Katz. Since the idea was never discussed in the briefs, Judge Schneider boldly articulated during his oral argument that "expectations of privacy should be based on an objective standard, one that could be formulated using the reasonable man standard from tort law."^[31] Realizing the significance of this new standard in its Fourth Amendment jurisprudence, Justice Harlan, in his own way, characterized the reasonable expectation of privacy test as "the rule that has emerged from prior decisions."^[32]

Justice Harlan expanded the test into its subjective and objective component, however, by stressing that the protection of the Fourth Amendment has a two-fold requirement: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'."^[33] Although the majority opinion in *Katz v. United States* made no reference to this reasonable expectation of privacy test, it instituted the doctrine that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."^[34]

In the 1968 case *Mancusi v. DeForte*,^[35] the US Supreme Court started to apply the reasonable expectation of privacy test pioneered by *Katz v. United States* and declared that the "capacity to claim the protection of the Amendment depends not upon a property right in the invaded place, but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion."^[36]

II

Bearing in mind the history and evolution of the right to privacy as a Constitutionally-protected right, I now dwell on whether the petitioner, a public employee, enjoyed an objective or reasonable expectation of privacy in his workplace, i.e. within the premises of respondent Civil Service Commission, his employer.

At the outset, I state that the right to privacy involved herein is the petitioner's right to informational privacy in his workplace, specifically his right to work freely without surveillance or intrusion.^[37]

I find relevant the doctrine laid down in *O'Connor v. Ortega*,^[38] where the US Supreme Court held that a person was deemed to have a lower expectation of privacy in his workplace. The decrease in expectation of privacy was not similar to a non-existent expectation, however, for the US Supreme Court clarified:

"Given the societal expectations of privacy in one's place of work expressed in both *Oliver* and *Mancusi*, we reject the contention made by the Solicitor General and petitioners that public employees can never have a reasonable expectation of privacy in their place of work. Individuals do not lose Fourth Amendment rights merely because they work for the government, instead of a private employer. The operational realities of the workplace, however, may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor, rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation. xxx An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others - such as fellow employees, supervisors, consensual visitors, and the general public - may have frequent access to an individual's office. We agree with JUSTICE SCALIA that

'[c]onstitutional protection against unreasonable searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer,'

but some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable.

xxxx

"Balanced against the substantial government interests in the efficient and proper operation of the workplace are the privacy interests of government employees in their place of work, which, while not insubstantial, are far less than those found at home or in some other contexts. As with the building inspections in *Camara*, the employer intrusions at issue here "involve a relatively limited invasion" of employee privacy. Government offices are provided to employees for the sole purpose of facilitating the work of an agency. The employee may avoid exposing personal belongings at work by simply leaving them at home. [emphasis supplied]

For sure, there are specific reasons why employees in general have a decreased expectation of privacy with respect to work-email accounts,^[39] including the following:

- (a) Employers have legitimate interests in monitoring the workplace;^[40]

(b) Employers own the facilities;

(c) Monitoring computer or internet use is a lesser evil compared to other liabilities, such as having copyright infringing material enter the company computers, or having employees send proprietary material to outside parties;

(d) An employer also has an interest in detecting legally incriminating material that may later be subject to electronic discovery;

(e) An employer simply needs to monitor the use of computer resources, from viruses to clogging due to large image or pornography files.[41]

In view of these reasons, the fact that employees may be given individual accounts and password protection is not deemed to create any expectation of privacy.[42]

Similarly, monitoring an employee's computer usage may also be impelled by the following legitimate reasons:

(a) To maintain the company's professional reputation and image;

(b) To maintain employee productivity;

(c) To prevent and discourage sexual or other illegal workplace harassment;

(d) To prevent "cyberstalking" by employees;

(e) To prevent possible defamation liability;

(f) To prevent employee disclosure of trade secrets and other confidential information; and

(g) To avoid copyright and other intellectual property infringement from employees illegally downloading software, etc.[43]

Even without Office Memorandum (OM) No. 10, Series of 2002 being issued by respondent Karina Constantino-David as Chairman of the Civil Service Commission, the employees of the Commission, including the petitioner, have a reduced expectation of privacy in the workplace. The objective of the issuance of OM No. 10 has been only to formally inform and make aware the employees of the Commission about the limitations on their privacy while they are in the workplace and to advise them that the Commission has legitimate reasons to monitor communications made by them, electronically or not. The objectives of OM No. 10 are, needless to state, clear in this regard.[44]

III

Unlike the Majority, I find that the petitioner did not absolutely waive his right to privacy.[45] OM No. 10 contains the following exception, to wit:

Waste of Computer Resources. x x x

x x x x

However, Users are given privileged access to the Internet for knowledge search, information exchange and others. They shall be allowed to use the computer resources for personal purpose after office hours provided that no unlawful materials mentioned in item number 7 and 8 are involved, and no other facilities such as air conditioning unit, video/audio system etc., shall be used except sufficient lights. [emphasis supplied]

Thereby, OM No. 10 has actually given the petitioner privileged access to the Internet for knowledge search, information exchange, and others; and has explicitly allowed him to use the computer resources for personal purposes after office hours. Implicit in such privileged access and permitted personal use was, therefore, that he

still had a reasonable expectation of privacy vis-à-vis whatever communications he created, stored, sent, or received after office hours through using the Commission's computer resources, such that he could rightfully invoke the Constitutional protection to the privacy of his communication and correspondence.

In view of the petitioner's expectation of privacy, albeit diminished, I differ from the Majority's holding that he should be barred from claiming any violation of his right to privacy and right against unreasonable searches and seizures with respect to all the files, official or private, stored in his computer. Although I concede that respondent David had legal authority and good reasons to issue her order to back up the petitioner's files as an exercise of her power of supervision, I am not in full accord with the Majority's holding for the confiscation of all the files stored in the computer. The need to control or prevent activities constitutionally subject to the State's regulation may not be filled by means that unnecessarily and broadly sweep and thereby invade the area of protected freedoms.[46]

I hold, instead, that the petitioner is entitled to a reasonable expectation of privacy in respect of the communications created, stored, sent, or received after office hours through the office computer, as to which he must be protected. For that reason, respondent David's order to back up files should only cover the files corresponding to communications created, stored, sent, or received during office hours. There will be no difficulty in identifying and segregating the files created, stored, sent, or received during and after office hours with the constant advancement and improvement of technology and the presumed expertise of the Commission's information systems analysts.

Nonetheless, my concurrence with the Majority remains as regards the petitioner's administrative liability and the seizure of the remainder of the files. I am reiterating, for emphasis, that the diminution of his expectation of privacy in the workplace derived from the nature and purpose of a government office, actual office practice and procedures observed therein, and legitimate regulation.[47] Thus, I vote to uphold the legality of OM No. 10. I hasten to add, to be very clear, that the validity of the seizure of the files should be limited to the need for determining whether or not the petitioner unjustly utilized official resources of the Commission for personal purposes, and should not extend to the reading of the files' contents, which would be violative of his right to privacy.

I adhere to the principle that every man is believed to be free. Freedom gears a man to move about unhampered and to speak out from conviction. That is why the right to privacy has earned its worthy place in the Bill of Rights. However, although the right to privacy is referred to as a right to be enjoyed by the people, the State cannot just sit back and stand aside when, in the exercise of his right to privacy, the individual perilously tilts the scales to the detriment of the national interest.

In upholding the validity of OM No. 10, I also suppose that it is not the intention of the Majority to render the Bill of Rights inferior to an administrative rule. Rather, adoption of the balancing of interests test, a concept analogous to the form of scrutiny employed by courts of the United States, has turned out to be applicable especially in the face of the conflict between the individual interest of the petitioner (who asserts his right to privacy) and the Commission's legitimate concern as an arm of the Government tasked to perform official functions. The balancing of interest test has been explained by Professor Kauper,[48] viz:

"The theory of balance of interests represents a wholly pragmatic approach to the problem of First Amendment freedom, indeed, to the whole problem of constitutional interpretation. It rests on the theory that is the Court's function in the case before it when it finds public interests served by legislation on the one hand and First Amendment freedoms affected by it on the other, to balance the one against the other and to arrive at a judgment where the greater weight shall be placed. If on balance it appears that the public interest served by restrictive legislation is of such a character that it outweighs the abridgment of freedom, then the Court will find the legislation valid. In short, the balance-of-interests theory rests on the basis that constitutional freedoms

are not absolute, not even those stated in the First Amendment, and that they may be abridged to some extent to serve appropriate and important interest." (emphasis supplied.)

The Court has applied the balancing of interest test in *Alejano v. Cabuay*,^[49] where it ruled that the substantial government interest in security and discipline outweighed a detainee's right to privacy of communication. The Court has elucidated:

"In *Hudson v. Palmer*, the U.S. Supreme Court ruled that an inmate has no reasonable expectation of privacy inside his cell. The U.S. Supreme Court explained that prisoners necessarily lose many protections of the Constitution, thus:

'However, while persons imprisoned for crime enjoy many protections of the Constitution, it is also clear that imprisonment carries with it the circumscription or loss of many significant rights. These constraints on inmates, and in some cases the complete withdrawal of certain rights, are "justified by the considerations underlying our penal system." The curtailment of certain rights is necessary, as a practical matter, to accommodate a myriad of "institutional needs and objectives" of prison facilities, chief among which is internal security. Of course, these restrictions or retractions also serve, incidentally, as reminders that, under our system of justice, deterrence and retribution are factors in addition to correction.'

"The later case of *State v. Dunn*, citing *Hudson v. Palmer*, abandoned *Palmigiano v. Travisono* and made no distinction as to the detainees' limited right to privacy. *State v. Dunn* noted the considerable jurisprudence in the United States holding that inmate mail may be censored for the furtherance of a substantial government interest such as security or discipline. *State v. Dunn* declared that if complete censorship is permissible, then the lesser act of opening the mail and reading it is also permissible. We quote *State v. Dunn*:

'[A] right of privacy in traditional Fourth Amendment terms is fundamentally incompatible with the close and continual surveillance of inmates and their cells required to ensure institutional security and internal order. We are satisfied that society would insist that the prisoner's expectation of privacy always yield to what must be considered a paramount interest in institutional security. We believe that it is accepted by our society that "[l]oss of freedom of choice and privacy are inherent incidents of confinement.'"

x x x x

"Thus, we do not agree with the Court of Appeals that the opening and reading of the detainees' letters in the present case violated the detainees' right to privacy of communication. The letters were not in a sealed envelope. The inspection of the folded letters is a valid measure as it serves the same purpose as the opening of sealed letters for the inspection of contraband.

x x x x

"In assessing the regulations imposed in detention and prison facilities that are alleged to infringe on the constitutional rights of the detainees and convicted prisoners, U.S. courts "balance the guarantees of the Constitution with the legitimate concerns of prison administrators." The deferential review of such regulations stems from the principle that:

[s]ubjecting the day-to-day judgments of prison officials to an inflexible strict scrutiny analysis would seriously hamper their ability to anticipate security problems and to adopt innovative solutions to the intractable problems of prison administration." [emphasis supplied]

Much like any other government office, the Commission was established primarily for the purpose of advancing and accomplishing the functions that were the object of its creation.^[50] It is imperative, therefore, that its resources be maximized to achieve utmost efficiency in order to ensure the delivery of quality output and services

to the public. This commitment to efficiency existed not solely in the interest of good government but also in the interest of letting government agencies control their own information-processing systems.[51] With the State and the people being the Commission's ultimate beneficiaries, it is incumbent upon the Commission to maintain integrity both in fact and in appearance at all times. OM No. 10 was issued to serve as a necessary instrument to safeguard the efficiency and integrity of the Commission, a matter that was of a compelling State interest, and consequently to lay a sound basis for the limited encroachment in the petitioner's right to privacy. But, nonetheless, Justice Goldberg's concurring opinion in *Griswold v. Connecticut*[52] might be instructive:

"In a long series of cases this Court has held that where fundamental personal liberties are involved, they may not be abridged by the States simply on a showing that a regulatory statute has some rational relationship to the effectuation of a proper state purpose. Where there is a significant encroachment upon personal liberty, the State may prevail only upon showing a subordinating interest which is compelling (*Bates v. Little Rock*, 361 U.S. 516, 524). The law must be shown `necessary, and not merely rationally related, to the accomplishment of a permissible state policy.'" (*McLaughlin v. Florida*, 379 U.S. 184, 186)

Even assuming that the anonymous tip about the petitioner's misuse of the computer proved to be false, i.e., the petitioner did not really engage in lawyering for or assisting parties with interests adverse to that of the Commission, his permitting former colleagues and close friends not officially connected with the Commission to use and store files in his computer,[53] which he admitted, still seriously breached, or, at least, threatened to breach the integrity and efficiency of the Commission as a government office. Compounding his breach was that he was well informed of the limited computer use and privacy policies in OM No. 10, in effect since 2002, prior to the seizure of his files in January of 2007. The Court should not disregard or ignore the breach he was guilty of, for doing so could amount to abetting his misconduct to the detriment of the public who always deserved quality service from the Commission.

IV

As early as in *Olmstead v. United States*,[54] Justice Brandeis anticipated the impact of technological changes to the right to privacy and significantly observed that -

"xxx time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. xxx"

In this era when technological advancement and the emergence of sophisticated methodologies in terms of the science of communication are already inexorable and commonplace, I cannot help but recognize the potential impact of the Majority's ruling on future policies to govern situations in the public and private workplaces. I apprehend that the ruling about the decreased expectation of privacy in the workplace may generate an unwanted implication for employers in general to henceforth consider themselves authorized, without risking a collision with the Constitutionally-protected right to privacy, to probe and pry into communications made during work hours by their employees through the use of their computers and other digital instruments of communication. Thus, the employers may possibly begin to monitor their employees' phone calls, to screen incoming and out-going e-mails, to capture queries made through any of the Internet's efficient search engines (like Google), or

to censor visited websites (like Yahoo!, Facebook or Twitter) in the avowed interest of ensuring productivity and supervising use of business resources. That will be unfortunate.

The apprehension may ripen into a real concern about the possibility of abuse on the part of the employers. I propose, therefore, that the ruling herein be made *pro hac vice*, for there may be situations not presently envisioned that may be held, wrongly or rightly, as covered by the ruling, like when the instrument of communication used is property not owned by the employer although used during work hours.

As a final note, let me express the sentiment that an employee, regardless of his position and of the sector he works for, is not a slave of trade expected to devote his full time and attention to the job. Although the interests of capital or public service do merit protection, a recognition of the limitations of man as a being needful of some extent of rest, and of some degree of personal space even during work hours, is most essential in order to fully maximize the potential by which his services was obtained in the first place. The job should not own him the whole time he is in the workplace. Even while he remains in the workplace, he must be allowed to preserve his own identity, to maintain an inner self, to safeguard his beliefs, and to keep certain thoughts, judgments and desires hidden. Otherwise put, he does not surrender his entire expectation of privacy totally upon entering the gates of the workplace. Unreasonable intrusion into his right to be let alone should still be zealously guarded against, albeit he may have waived at some point a greater part of that expectation. At any rate, whenever the interest of the employer and the employee should clash, the assistance of the courts may be sought to define the limits of intrusion or to balance interests.

ACCORDINGLY, I vote to deny the petition, subject to the qualification that the petitioner's right to privacy should be respected as to the files created, stored, sent or received after office hours; and to the further qualification that the decision be held to apply *pro hac vice*.

[1] 4 Harvard Law Review 193.

[2] Richards, Neil M. and Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, The Georgetown Law Journal, Vol. 96 (2007), pp. 128-129.

[3] *Supra*, note 1, p. 198.

[4] *Id.*, p. 195; Warren and Brandeis adopted the "right to be let alone" language from Judge Thomas M. Cooley's 1888 treatise *The Law of Torts* 29 (2d ed. 1888).

[5] Richards and Solove, *op. cit.*, p. 125.

[6] 277 U.S. 438 (1928).

[7] 48 California Law Review, No. 3 (August 1960), p. 383.

[8] *Id.*, p. 389.

[9] *Id.*; see also Richards and Solove, *op. cit.*, pp. 148-149.

[10] Restatement of Torts 2d §652B (1977) (Prosser was also a reporter of the Second Restatement of Torts).

[11] *Id.*, §652D-§652E (1977).

[12] *Id.*, §652C (1977.)

[13] 429 U.S. 589 (1977).

[14] Gilbert, Helen L., Minors' Constitutional Right to Informational Privacy, The University of Chicago Law Journal (2007), pp. 1385-1386.

[15] Id., p. 1386.

[16] 638 F2d 570 (3d Cir 1980).

[17] Id., p. 578.

[18] 262 U.S. 390 (1923).

[19] The criminal information was based upon "An act relating to the teaching of foreign languages in the State of Nebraska," approved April 9, 1919, pertinent portions of which provide:

Section 1. No person, individually or as a teacher, shall, in any private, denominational, parochial or public school, teach any subject to any person in any language other than the English language.

Sec. 2. Languages, other than the English language, may be taught as languages only after a pupil shall have attained and successfully passed the eighth grade as evidenced by a certificate of graduation issued by the county superintendent of the county in which the child resides.

Sec. 3. Any person who violates any of the provisions of this act shall be deemed guilty of a misdemeanor and upon conviction, shall be subject to a fine of not less than twenty-five dollars (\$25), nor more than one hundred dollars (\$100) or be confined in the county jail for any period not exceeding thirty days for each offense.

Sec. 4. Whereas, an emergency exists, this act shall be in force from and after its passage and approval.

[20] 381 U.S. 479 (1965).**[21] 410 U.S. 113 (1973)**

[22] A.M. No. P-02-1651, August 4, 2003, 408 SCRA 1.

[23] Bernas, Joaquin G., The 1987 Constitution of the Philippines, 1986 Ed., p. 191.

[24] 410 U.S. 113 (1973).

[25] Ninth Amendment of the United States Constitution.

[26] G.R. No. L-20387, 22 SCRA 424, January 31, 1968.

[27] Id., citing Public Utilities Commission v. Pollak, 343 U. S. 451, 467 (1952).

[28] 277 U.S. 438 (1928).**[29] 389 U.S. 347, 350-351 (1967).**

[30] The transcript of Judge Schneider's oral argument in part provides:

Mr. Schneider: x x x We think and respectfully submit to the Court that whether or not, a telephone booth or any area is constitutionally protected, is the wrong initial inquiry.

We do not believe that the question should be determined as to whether or not, let's say you have an invasion

of a constitutionally protected area, that shouldn't be the initial inquiry, but rather that probably should be the conclusion that is reached after the application of a test such as that we propose are similar test.

Now, we have proposed in our brief and there's nothing magical or ingenious about our test.

It's an objective test which stresses the rule of reason, we think.

The test really asks or opposes the question, "Would a reasonable person objectively looking at the communication setting, the situation and location of a communicator and communicatee -- would he reasonably believe that that communication was intended to be confidential?"

We think that in applying this test there are several criteria that can be used.

Justice William J. Brennan: So that parabolic mic on the two people conversing in the field a mile away might --

Mr. Schneider: Absolutely.

x x x

We think that if a confidential communication was intended and all the other aspects of confidentiality are present, then it makes no difference whether you're in an open field or in the privacy of your own home.

We would submit to the Court that there are factors present which would tend to give the Courts, the trial courts, and ultimately this Court, some guidelines as to whether or not objectively speaking, the communication was intended to be private.

x x x

Mr. Schneider: x x x

I believe the following factors at least should be included in an analysis of this problem.

One, what is the physical location?

In other words, where did the conversation take place?

Was it in a situation where numerous persons were present or whether just a few people present?

I think that bears on the issue.

I think the tone of voice bears on the issue.

I think that you can have a communication for example in your house which almost everyone would see all things being equal would be confidential.

However, if you use a loud enough voice, I think you destroy your own confidentiality.

x x x

Mr. Schneider: x x x

We feel that the Fourth Amendment and at the Court's decisions recently for a long time, I believe, have indicated that the right to privacy is what's protected by the Fourth Amendment.

We feel that the right to privacy follows the individual.

And that whether or not, he's in a space when closed by four walls, and a ceiling, and a roof, or an auto-mobile, or any other physical location, is not determined of the issue of whether or not the communication can

ultimately be declared confidential.

x x x

Justice John M. Harlan: Could you state this Court tested this as you propose?

Mr. Schneider: Yes, we propose a test using in a way it's not too dissimilar from a tort, that tort reasonable man test.

We're suggesting that what should be used is the communication setting should be observed and those items that should be considered are the tone of voice, the actual physical location where the conversation took place, the activities on the part of the officer.

When all those things are considered, we would ask that the test be applied as to whether or not a third person objectively looking at the entire scene could reasonably interpret and could reasonably say that the communicator intended his communication to be confidential. x x x (emphasis supplied.)

[31] Winn, Peter, Katz and the Origins of the "Reasonable Expectation of Privacy" Test, 2008.

[32] Id.; see the concurring opinion of Justice Harlan in *Katz v. United States*, 389 U.S. 347, 350-351 (1967).

[33] Concurring opinion of Justice Harlan in *Katz v. United States*, supra.

[34] *Katz v. United States*, supra; writing for the majority, Justice Stewart made the following pronouncement:

xxx. In the first place, the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy -- his right to be let alone by other people -- is, like the protection of his property and of his very life, left largely to the law of the individual States.

[35] 392 U.S. 364 (1968).

[36] Justice Harlan delivered the opinion of the Court.

[37] In *Whalen v. Roe*, supra, note 13, p. 599, the Court advanced the principle that the right to information privacy has two aspects: (1) the right of an individual not to have private information about himself disclosed; and (2) the right of an individual to live freely without surveillance and intrusion.

[38] 480 U.S. 709, 715-17 (1987).

[39] Tan, Oscar Franklin B., Articulating the Complete Philippine Right to Privacy in Constitutional and Civil Law: A Tribute to Chief Justice Fernando and Justice Carpio, *Philippine Law Journal*, Vol. 82, No. 4 (2008), pp. 228-229.

[40] Id., citing Michael Rustad and Thomas Koenig, *Cybertorts and Legal Lag: An Empirical Analysis*, 13 S. Cal. Interdisc. L.J. 77, 95 (2003).

[41] Id., citing Matthew Finkin, *Information Technology and Worker's Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002).

[42] Supra Note 6, p. 228.

[43] Ciocchetti, Corey A., Monitoring Employee Email: Efficient Workplaces vs. Employee Privacy, <<http://www.law.duke.edu/journals/dltr/articles/2001dltr0026.html#8>> Last visited on June 14, 2011; citing Terrence Lewis, Pittsburgh Business Times, Monitoring Employee E-Mail: Avoid stalking and Illegal Internet Conduct).

[44] Rollo, p. 98.

O.M. No. 10 provides:

OBJECTIVES

Specifically, the guidelines aim to:

- Protect confidential, proprietary information of the CSC from theft or unauthorized disclosure to third parties;
- Optimize the use of the CSC's Computer Resources as what they are officially intended for; and
- Reduce, and possibly eliminate potential legal liability to employees and third parties.

[45] Id., p. 99; O.M. No. 10 states:

Waiver of privacy rights. Users expressly waive any right to privacy in anything they create, store, send, or receive on the computer through the Internet or any other computer network. Users understand that the CSC may use human or automated means to monitor the use of its Computer Resources.

[46] *Griswold v. Connecticut*, supra, note 20, citing *NAACP v. Alabama*, 377 U.S. 288 (1964).

[47] *O'Connor v. Ortega*, 25 480 U.S. 709, 715-17 (1987).

[48] Cited in *Gonzales v. COMELEC*, G.R. No. L-27833, April 18, 1969, 27 SCRA 835, 899.

[49] G.R. No. 160792, August 25, 2005, 468 SCRA 188, 211-214.

[50] The Civil Service Commission was conferred the status of a department by Republic Act No. 2260 as amended and elevated to a constitutional body by the 1973 Constitution. It was reorganized under PD No. 181 dated September 24, 1972, and again reorganized under Executive Order no. 181 dated November 21, 1986. With the new Administrative Code of 1987 (EO 292), the Commission is constitutionally mandated to promote morale, efficiency, integrity, responsiveness, progressiveness, and courtesy in the Civil Service. Also, as the central human resource institution and as adviser to the President on personnel management of the Philippine Government, the Civil Service Commission exists to be the forerunner in (1) upholding merit, justice and fairness; (2) building competence, expertise and character; (3) ensuring delivery of quality public services and products; (4) institutionalizing workplace harmony and wellness; and (5) fostering partnership and collaboration. www.csc.gov.ph/mandate and mission. Last visited on July 13, 2011.

[51] Regan, Priscilla M., *Legislating Privacy (Technology, Social Values, and Public Policy)*, The University of North Carolina Press, 1995, p. 186.

[52] 381 U.S. 479 (1965).

[53] Rollo, p. 96-97; Paragraphs 4 and 5 of the Affidavit executed by Ponciano R. Solosa narrated the following:

4. That I have also requested Ricky who is like a son to me having known him since he was eighteen (18) years old, to keep my personal files for safekeeping in his computer which I understand was issued thru Memorandum Receipt and therefore for his personal use;

5. That this affidavit is issued to attest to the fact that Mr. Pollo has nothing to do with my files which I have entrusted to him for safekeeping including my personal pleadings with the LTO and PUP, of which I have been the counsel on record and caused the preparation and signed thereof accordingly.

Also, paragraph 5 of the Affidavit executed by Eric N. Estrellado mentioned the following:

8. That I deny what was indicated in CSC Resolution No. 07-0382 under item 13 and 14 that Ricky Pollo is earning out of practicing or aiding people undersigned included, the truth of the matter the statement made "Epal, kulang ang bayad mo.", was a private joke between me and my counsel and friend Atty. Solosa. That item 14 was my billing statement with the law firm of solosa [sic] and de Guzman. Ricky has nothing to do with it. These private files but was intruded and confiscated for unknown reasons by people who are not privy to our private affairs with my counsel. That these are in the CPU of Ricky, as he would request as in fact Atty. Solosa himself requested Ricky to keep files thereof thru flash drive or disk drive;

[54] Dissenting Opinion of Justice Brandeis, *Olmstead v. United States*, supra Note 6.

SEPARATE CONCURRING OPINION

CARPIO, J.:

I concur with the Court's denial of the petition. However, I file this separate opinion to (1) assert a statutory basis for the disposition of the case, and (2) articulate the exception to the Civil Service Commission (CSC) office regulation denying expectation of privacy in the use of government computers.

First. The CSC's computer use regulation, which opens to access for internal scrutiny anything CSC employees "create, store, send, or receive in the computer system," has a statutory basis under the Government Auditing Code of the Philippines. Section 4(2) of the Code mandates that "[g]overnment x x x property shall be x x x used solely for public purposes."^[1] In short, any private use of a government property, like a government-owned computer, is prohibited by law. Consequently, a government employee cannot expect any privacy when he uses a government-owned computer because he knows he cannot use the computer for any private purpose. The CSC regulation declaring a no-privacy expectation on the use of government-owned computers logically follows from the statutory rule that government-owned property shall be used "solely" for a public purpose.

Moreover, the statutory rule and the CSC regulation are consistent with the constitutional treatment of a public office as a public trust.^[2] The statutory rule and the CSC regulation also implement the State policies, as expressly provided in the Constitution, of ensuring full disclosure of all government transactions involving public interest,^[3] maintaining honesty and integrity in the public service, and preventing graft and corruption.^[4]

Thus, in this jurisdiction, the constitutional guarantees of privacy and reasonable search are unavailing against audit inspections or internal investigations for misconduct, as here, of electronic data stored in government-owned property such as computing, telecommunication, and other devices issued to civil servants. These constitutional guarantees apply only to searches of devices privately owned by government employees.

Second. The CSC office regulation denying CSC employees privacy expectation in "anything they create, store, send, or receive in the computer system,"^[5] although valid as to petitioner Briccio Pollo, is constitutionally infirm insofar as the regulation excludes from its ambit the three CSC commissioners solely by reason of their rank, and not by reason of the confidential nature of the electronic data they generate.

Office regulations mandating no-privacy expectation such as the CSC regulation in question cannot justify access

to sensitive government information traditionally recognized as confidential. Thus, insulated from the reach of such regulations are Presidential conversations, correspondences, or discussions during closed-door Cabinet meetings, internal deliberations of the Supreme Court and other collegiate courts, draft decisions of judges and justices, executive sessions of either house of Congress, military and diplomatic secrets, national security matters, documents relating to pre-prosecution investigations by law enforcement agencies and similar confidential matters.[6] The privilege of confidentiality covering these classes of information, barring free access to them, is grounded on the nature of the constitutional function of the public officials involved, coupled with considerations of efficiency, safety and comity interests since disclosure of confidential information jeopardizes decision-making, endangers lives and undermines diplomatic dealings, as the case may be.

The CSC, as the government's "central personnel agency,"[7] exercises quasi-judicial functions in "[r]ender[ing] opinion and rulings on all personnel and other Civil Service matters." [8] The CSC's internal deliberations on administrative cases are comparable to the internal deliberations of collegial courts. Such internal deliberations enjoy confidentiality and cannot be accessed on the ground that an audio of the deliberations is stored in a government-owned device. Likewise, draft decisions of CSC commissioners that are stored in government-issued computers are confidential information.

By providing that "[u]sers except the Members of the Commission shall not have an expectation of privacy in anything they create, store, send, or receive in the [government-owned] computer system," the CSC regulation creates a new, constitutionally suspect category of confidential information based, not on the sensitivity of content, but on the salary grade of its author. Thus, a glaring exemption from the CSC's own transparency regulation is "anything x x x create[d], store[d], sen[t], or receive[d]" in the commission's computer system by the three CSC members. As the new category is content-neutral and draws its confidentiality solely from the rank held by the government official creating, storing, sending and receiving the data, the exemption stands on its head the traditional grounding of confidentiality - the sensitivity of content.

The constitutional infirmity of the exemption is worsened by the arbitrariness of its rank-based classification. The three CSC commissioners, unlike the rest of the lower ranked CSC employees, are excluded from the operation of the CSC's data transparency regulation solely because they are the CSC's highest ranking officers.[9] This classification fails even the most lenient equal protection analysis. It bears no reasonable connection with the CSC regulation's avowed purposes of "[1] [p]rotect[ing] confidential, proprietary information of the CSC from theft or unauthorized disclosure to third parties; [2] [o]ptimiz[ing] the use of the CSC's [c]omputer [r]esources as what they are officially intended for; and [3] [r]educ[ing] and possibly eliminat[ing] potential legal liability to employees and third parties." [10] The assumption upon which the classification rests - that the CSC commissioners, unlike the rest of the CSC's thousands of employees, are incapable of violating these objectives - is plainly unfounded.

The only way by which the CSC commissioners, or for that matter, any of its employees, can constitutionally take themselves out of the ambit of the CSC's no-privacy regulation is if they (1) invoke the doctrine of confidentiality of information, and (2) prove that the information sought to be exempted indeed falls under any of the classes of confidential information adverted to above (or those comparable to them). Sensitivity of content, not rank, justifies enjoyment of this very narrow constitutional privilege.

Accordingly, I vote to DENY the petition.

[1] Presidential Decree No. 1445. Section 4(2) provides in full: "Government funds or property shall be spent or used solely for public purposes."

[2] Section 1, Article XI of the Constitution provides: "Public office is a public trust. Public officers and employees must, at all times, be accountable to the people, serve them with utmost responsibility, integrity, loyalty, and efficiency; act with patriotism and justice, and lead modest lives."

[3] Section 28, Article II of the Constitution provides: "Subject to reasonable conditions prescribed by law, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest."

[4] Section 27, Article II of the Constitution provides: "The State shall maintain honesty and integrity in the public service and take positive and effective measures against graft and corruption."

[5] The rule under CSC Memorandum No. 10, series of 2002, provides:

No expectation of privacy. Users except the Members of the Commission shall not have expectation of privacy in anything they create, store, send or receive in the computer system.

The Head of the Office for Recruitment, Examination and Placement shall select and assign Users to handle the confidential examination of data and processes.

[6] Under *Chavez v. Public Estates Authority* (G.R. No. 133250, 9 July 2002, 384 SCRA 152, 188), these are also beyond the reach of the constitutional right to information.

[7] Constitution, Article IX(B), Section 3.

[8] Executive Order No. 292, Book V, Title I, Chapter 3, Section 12(5).

[9] Aside from its three commissioners, the CSC has two assistant commissioners and twelve divisions in its central office, including an office for legal affairs. The CSC also maintains 16 regional offices.

[10] CSC Memorandum No. 10, series of 2002, enumerates these as its objectives.

ABOUT BATAS.ORG

Study smarter at BATAS.org

The Philippine bar review and law-school companion built around how your brain actually remembers.

The complete Philippine law library - free for everyone.

More than 100,000 Supreme Court decisions, Republic Acts, and executive issuances - full-text searchable, browsable by category and year, and always free. No paywall, no login. This PDF came from it.

Audio case-brief lectures.

Any decision becomes a podcast-style lecture - facts, issues, ruling, and doctrine - with read-along highlighting and a hands-free presentation mode. Study while commuting, working out, or resting your eyes.

Bar review built on the science of memory.

Complete, sequenced courses for all eight bar subjects, narrated like podcasts and reinforced with retrieval practice and spaced review - the study techniques with the strongest evidence behind them.

The full law-school curriculum.

One subscription unlocks the entire J.D. curriculum - every subject, every lesson, with your progress tracked down to the paragraph so you can pick up exactly where you left off, on any device.

Mock exams that tell you where you stand.

Timed multiple-choice exams graded instantly, with per-subject score breakdowns and focus suggestions that point you at your weakest topics first.

A study planner that keeps you on pace.

Set your schedule and BATAS tells you every day whether you are on track for bar day - and exactly which lesson to take next.

Start free at <https://batas.org>

The law library is free forever - and your first lesson is one click away.

The text of this document is an official public record and remains in the public domain. Formatting, presentation, and compilation © 2026 batas.org.

Downloaded free from the batas.org Law Library. Share it freely - the library is free for every law student, bar reviewee, and practitioner.